View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Biblioteca Digital Jurídica do Superior Tribunal de Justiça

Revista Electrónica de Ciencia Penal y Criminología

RECPC 01-14 (1999)

PROTECCIÓN PENAL DE SISTEMAS, ELEMENTOS, DATOS, DOCUMENTOS Y PROGRAMAS INFORMÁTICOS

Juan José González Rus

Catedrático de Derecho Penal
Universidad de Córdoba

El presente trabajo constituye una versión revisada de la ponencia presentada en las Jornadas sobre delincuencia informática, celebradas en el Centro de Estudios Jurídicos de la Administración de Justicia durante los días 2 al 4 de junio de 1997. Respecto del texto provisional de la ponencia (publicado en Estudios Jurídicos. Ministerio Fiscal. III., Madrid, 1997), es completamente nueva la parte relativa al tratamiento penal de los programas de ordenador.

SUMARIO:

I. DELITOS "INFORMÁTICOS" DE NATURALEZA PATRIMONIAL Y ECONÓMICA. CONSIDERACIONES GENERALES Y CLASIFICACIÓN DE LOS COMPORTAMIENTOS PUNIBLES

El Código penal de 1995 incorpora previsiones específicas relacionadas directamente con comportamientos que tienen a sistemas o a elementos informáticos como objeto de ataque o como instrumento del delito. Con ello se pretende llenar las lagunas de punición que presentaba el Código penal anterior, en el que resultaban atípicos la mayor parte de los hechos de este tipo (1). El camino seguido ha sido el de complementar tipos legales ya existentes, en los que se han introducido especificaciones sobre la conducta típica (estafa) o el objeto material (daños) (2). De esta forma, se ha atendido la demanda doctrinal mantenida insistentemente durante los últimos años y se intenta dar respuesta penal adecuada a formas de criminalidad nuevas (3), que son ya una realidad y que en el futuro inmediato tendrán una incidencia aún mayor.

Dejando aparte las lesiones a la intimidad, que no serán tratadas aquí (4), los comportamientos relacionados con medios o procedimientos informáticos que pueden alcanzar relevancia penal son muy variados. Las formas de comisión posibles son tantas y tan diversas y las figuras delictivas que pueden verse implicadas tan distintas (hurto, robo, estafa, daños, falsificaciones, descubrimiento de secretos de empresa, utilización ilegítima de terminales de telecomunicación, defraudaciones de la propiedad intelectual, etc.) que los intentos de clasificación resultan particularmente complicados. Un mismo procedimiento comisivo puede dar lugar, según los casos, a diversos tipos de fraude o manipulación, pudiendo ser analizado desde la perspectiva de varios y distintos delitos, según la ocasión; del mismo modo que, en otras, el uso de la informática no supone más que un modus operandi nuevo que no plantea particularidad alguna respecto de las formas tradicionales de comisión.

Así, por recordar algunos procedimientos y ayudar a situar la cuestión, la técnica del caballo de Troya (5), el acceso no autorizado a sistema mediante el denominado hacking (6), el superzaping (7), el scavengning (8), la utilización de puertas falsas (9) o la entrada a cuestas (10), pueden servir para provocar, según los casos, cálculos y resultados erróneos en la ejecución de programas y aplicaciones, transferencias electrónicas de fondos, destrucción o inutilización de ficheros, modificación de programas, de datos o de documentos electrónicos, apoderamiento de ficheros o programas o el descubrimiento de secretos industriales o de empresa (11). Por eso que las distintas clasificaciones que se han propuesto resulten, en mayor o menor grado, objetables (12).

En términos generales, creo que sigue siendo válida la sistemática que sin pretensiones clasificatorias propusiera en su día (13), y que diferencia entre los hechos en los que el sistema informático o sus elementos son el objeto material del delito y aquéllos otros en los que son el instrumento del mismo. En el primer caso, delitos contra el sistema informático o contra elementos de naturaleza informática se incluyen los comportamientos en los que cualquiera de estos componentes (tanto físicos -hardware- como lógicos -software y ficheros y archivos) (14) resulta el objeto material de ilícitos patrimoniales, bien porque son en sí objeto específico de protección (terminales de comunicación, programas de ordenador, datos, informaciones, documentos electrónicos) bien porque pueden servir de soporte a elementos protegidos de manera general, pero en los que la aparición de implicaciones informáticas puede plantear peculiaridades dignas de atención específica (secretos de empresa, obras literarias o artísticas, datos con eventual valor probatorio recogidos en ficheros informáticos, etc.). En todo caso, diferenciando entre los delitos contra elementos físicos, que no plantean realmente problemas significativos, y los que afectan a elementos lógicos, cuya naturaleza suscita concretas y muy interesantes cuestiones.

En el segundo grupo se incluyen, en cambio, los delitos que se realizan por medio del sistema informático o utilizando elementos de naturaleza informática, que aparecen como el instrumento

utilizado para la realización del ilícito patrimonial o socioeconómico. Ello, tanto si el objeto de ataque es un elemento patrimonial cualquiera (dinero, en caso de las transferencias electrónicas de fondos o en la utilización de tarjetas de cajeros automáticos, por ejemplo) como cuando es también un sistema informático (introducción de virus, acceso ilícito a ordenadores y redes, etc.). En muchos supuestos concurrirán ambas perspectivas (daños a un sistema informático accediendo ilícitamente al mismo), lo que, en su caso, podrá dar lugar a eventuales concursos de delitos y hará preferente la contemplación desde la óptica de los delitos contra el sistema informático. Salvo que presenten problemas específicos, ningún comentario se hará cuando los medios informáticos sean simplemente una forma más de cometer delitos, sin que ello añada particularidad alguna al hecho (daños en una cadena de montaje, alterando el programa del ordenador que la controla, por ejemplo).

En lo que sigue se analiza el tratamiento penal que reciben los distintos supuestos. Las referencias a las figuras delictivas eventualmente aplicables se limitarán a los aspectos que guardan relación directa con la protección de sistemas, elementos, datos, documentos y programas informáticos. No se hará, pues, un comentario general de cada uno de los delitos, sino que se dará por supuesto -remitiendo, en su caso, a bibliografía complementaria-, el conocimiento de aquéllos que no guardan una relación directa con los temas que tratamos o cuya interpretación no ofrece particularidad especial alguna desde la perspectiva de la materia que nos ocupa.

II. DELITOS CONTRA EL SISTEMA INFORMÁTICO

Los delitos contra sistemas informáticos que afectan a elementos físicos del mismo no ofrecen particularidades dignas de mención respecto de comportamientos semejantes que se dirigen contra otros objetos. Tanto el hurto (art. 234) como el robo (arts. 237, 238 y 242), la estafa (art. 248.1) o la apropiación indebida (art. 252) se aplicarán conforme a los criterios interpretativos propios de cada uno de ellos. Lo mismo sucede con los ficheros de información o con los programas contenidos en los soportes de almacenamiento masivo cuando es sobre el objeto físico en el que se encuentran grabados (disquete, cinta, "disco duro", CD-rom, etc.) sobre el que recae la conducta delictiva. El valor económico a computar para la apreciación del delito o la falta será, en este caso, el que resulte del importe de uno y otro (15). Del mismo modo, tampoco ofrece particularidad alguna la aplicación de los delitos relativos a la propiedad industrial (arts. 273 a 277), cuando se produzcan lesiones de patentes, modelos de utilidad, modelos o dibujos industriales, topografías de un producto semiconductor, marcas, etc. (16).

Absolutamente distinto es el panorama que ofrecen los comportamientos relacionados con los elementos lógicos del sistema cuando las conductas afecten exclusivamente a los ficheros o programas, sin incidencia alguna en los elementos físicos del sistema informático. Aunque las conductas pueden producirse también por medios físicos (destrucción de un fichero de datos rompiendo el disco en el que se recoge, acercar un imán, etc.), por lo general los comportamientos con eventual relevancia penal se llevarán a cabo exclusivamente mediante procedimientos informáticos, copiando, borrando, manipulando, accediendo ilícitamente al sistema, transmitiendo la información o las instrucciones que contienen los datos, los ficheros o los programas afectados.

El tratamiento penal de estos supuestos depende de la conducta que se realice y del tipo de datos o ficheros que se vean afectados. Las posibilidades que pueden darse en la práctica son muy variadas, por lo que para abordar el tratamiento penal de los distintos casos distinguiremos los siguientes apartados:

1. Conductas que suponen el borrado, la alteración o la inutilización de datos, programas o documentos electrónicos, y que-cualquiera que sea el contenido del fichero- deben ser analizadas desde la perspectiva de los daños. En este apartado, que se denomina comúnmente sabotaje informático, incluiremos también los daños en los propios sistemas o elementos físicos del mismo (vid. infra II.1).

2. Conductas que suponen lo que genéricamente podría llamarse acceso ilícito a sistemas informáticos. Como la finalidad perseguida con ello puede ser muy diversa, dentro de la categoría pueden incluirse tanto supuestos de lo que acostumbra a denominarse espionaje informático (vid.infra II.2.A) como el apoderamiento de datos, ficheros y programas (vid.infra II.2.B) e incluso los daños, cuando ello sea el fin que se pretenda y se cause. Si el acceso ilegítimo es la vía utilizada para obtener un beneficio patrimonial propio o de tercero (ordenando transferencias electrónicas de fondos, por

ejemplo) el hecho se analizará en los delitos cometidos a través del sistema informático (vid.infra III).

3. Piratería de programas de ordenador, que debe ser analizadas desde la óptica de la propiedad intelectual (vid. infra II.3).
4. Utilización ilegítima de sistemas o elementos informáticos, modalidad de uso prevista expresamente para los terminales de comunicación en el art. 256 (vid.infra II.4).

1. Daños en sistemas o elementos informáticos y en datos, programas o documentos electrónicos (Sabotaje informático)

La destrucción de sistemas informáticos y de datos, programas y documentos electrónicos es uno de los comportamientos más frecuentes y de mayor gravedad en el ámbito informático (17). El daño puede afectar tanto a los elementos físicos del sistema (destrucción de un monitor, incendio de una unidad de proceso, inutilización de una impresora, etc.) como a los elementos lógicos. En el primer caso, el tratamiento penal no ofrece particularidad alguna, debiendo aplicarse el tipo básico de daños del art. 263, y eventualmente las agravaciones del art. 264 (18), cuando los daños afecten exclusivamente a objetos físicos del sistema. Cuando los daños alcancen también a elementos lógicos será aplicable, como veremos, la figura agravada del art. 262.2 (19).

Los supuestos que resultan más complicados desde el punto de vista penal son, pues, los de destrucción de datos, programas o documentos electrónicos, que son, además, los que han alcanzado mayor notoriedad. Aunque los daños pueden producirse tanto por procedimientos físicos (20) como propiamente informáticos, son éstos los que despiertan mayor interés. La proliferación de virus (21), bombas lógicas (22) y procedimientos similares (23) ha despertado tal preocupación que algunos ordenamientos han previsto expresamente la difusión de los mismos (24). A esa preocupación responde el art. 264.2, introducido por el Código penal de 1995 y en el que se recoge como modalidad agravada de daños la conducta de quien «por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos» (prisión de uno a tres años y multa de doce a veinticuatro meses).

Aunque ya en el Código anterior nada se oponía a la aplicación del delito a este tipo de elementos, con esta previsión el Código zanja la polémica en torno a la aplicación de los daños a los datos y elementos informáticos, negada para el Código anterior por la doctrina mayoritaria (25). Ello suponía expulsar del delito a ficheros, programas y aplicaciones y elementos lógicos de redes, soportes o sistemas informáticos, de gran valor económico y que, en cuanto impulsos electromagnéticos, son -de acuerdo con el sentido tradicional de la "corporalidad"- incorporales, aunque tienen un valor autónomo e independiente del que corresponde al soporte magnético en el que se graban. Lo cierto es que los datos son entidades físicas y, en ese sentido, materiales, aunque no sean en sí aprehensibles ni perceptibles de manera inmediata por los sentidos (26). Sin embargo, sí pueden ser directamente dañados, y por ello objeto material del delito de daños, condición que corresponde a la cosa corporal o incorporal, mueble o inmueble, económicamente valorable, susceptible de deterioro o destrucción y de ejercicio de la propiedad (27).

En todo caso, la previsión expresa resulta oportuna, en la medida en que resuelve las dudas que, por más que resultaran infundadas, pudieran mantenerse al respecto (28). Que la conducta se conciba como modalidad agravada de daños evidencia, además, que se les da más importancia que a los propios elementos físicos del sistema informático, cuya afectación daría lugar al tipo básico del art. 263.

De acuerdo con la prosa legal, el objeto material del delito viene dado, pues, por «datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos». La característica común a todos ellos es que no pueden ser leídos o percibidos directamente por el hombre, precisándose para ello la ayuda de máquinas capaces de interpretar las señales digitales que los integran (29). «Datos» son las unidades básicas de información, cualquier que sea su contenido (un número, una palabra, un sonido, una imagen) y que al ser procesadas dan lugar a la "información", que resulta de la conexión entre dos o más datos (30) y que a pesar de no ser mencionada expresamente en el precepto debe considerarse también incluida. «Programas» son la secuencia de instrucciones que se utilizan para el procesamiento de los datos con vistas a la realización de tareas específicas. En la secuencia legal, la referencia a «documentos electrónicos» parece estar reservada a aquéllos en los que se recogen los resultados del procesamiento de los datos

obtenidos con las distintas aplicaciones. Por lo demás, -y salvo lo que después se dirá respecto de la existencia de copias de seguridad- es indiferente que en el momento de la conducta se encuentren recogidos en memoria central o en soporte magnético. Así lo resalta el precepto al aludir a que pueden estar recogidos en redes, soportes o sistemas informáticos (31). Por lo demás, pueden.

La exigencia de "ajenidad" de los datos hace que el propietario no pueda ser sujeto activo del delito. Sin embargo, la determinación de a quién pertenecen en exclusiva los datos en relación con elementos en los que es frecuente el uso y la elaboración compartida puede presentar delicados problemas que deben ser resueltos conforme a la normativa civil correspondiente (32).

La formulación de la conducta típica plantea todas las dudas que son consubstanciales al concepto de daños, cuya determinación, pese a la aparente simplicidad del término, es polémica. Centrando la cuestión en los elementos lógicos, penalmente hablando, dañar es equivalente a destruir, deteriorar, inutilizar o alterar una cosa. Por lo menos así los concibe expresamente el art. 264.2 con una formulación tan amplia que hace que tales modalidades de conducta aparezcan como formas de dañar los datos, programas o documentos electrónicos, aceptando implícitamente la posibilidad de que pueda haber otros.

Además, en los daños se discute, como es sabido, de una parte, si para que puedan integrarse es preciso o no que se altere la sustancia de la cosa; de otra, si es necesaria o no la causación de un perjuicio patrimonial efectivo al sujeto pasivo; cuestiones todas que adquieren matices propios en relación con datos, programas y documentos electrónicos como consecuencia de la especificidad de los elementos informáticos.

Con relación al primer asunto, se ha considerado que el delito de daños implica que se afecte la esencia o sustancia de la cosa, de manera que no serían constitutivos de delito los casos en los que, permaneciendo inalterada la estructura material del objeto, sólo se lesiona el valor de uso que la cosa tiene para el propietario (33). El sector doctrinal mayoritario, por el contrario, mantiene la existencia del delito cuando se priva al propietario del uso a que aparecía destinada la cosa dañada; entre otras razones, porque se considera que una tal exigencia no se contiene en el Código, y porque las referencias a la inutilización (arts. 264.2 y 265) acogen los casos en los que simplemente se destruye el valor de uso (34).

Personalmente, creo que no son infundadas las limitaciones que tratan de imponerse al delito de daños al exigir que la conducta suponga algo más que la simple afectación del valor de uso de la cosa. Y es que aceptar sin más que la sola destrucción del valor de uso configura los daños se corresponde mal con los criterios vigentes en el Título XIII en torno a la punición de las infracciones de uso, ciertamente restrictivos, sin que parezca muy lógico entender que, con excepción de los vehículos a motor y el uso de terminales de telecomunicación, expresamente previstos, el único caso en el que de manera genérica se protege penalmente la privación del uso sea en los daños. Por otra parte, la definición del delito, aunque sucinta, resalta la necesidad de que se produzcan daños «en propiedad ajena», lo que tampoco se corresponde bien con la simple afectación del uso, que aún siendo uno de los aspectos que la definen no es, sin embargo, el más identificativo de la misma. Todo ello, sin olvidar que el término «inutilización» es perfectamente congruente con la exigencia de que en los daños se produzca algún tipo de incidencia material en la estructura del objeto.

En atención a todo ello, me parece necesario requerir una afectación de la sustancia, que determine, aún de forma mínima, un menoscabo de la cosa que tiene incidencia en su propia existencia y suponga una pérdida de valor real independiente de los perjuicios derivados de la imposibilidad de uso, comprendiendo, en todo caso, los supuestos de pérdida, corrupción o degradación del objeto, así como los de alteración o inutilización (35).

A ello debe añadirse que la determinación de la cuantía conforme a la que tipificar el hecho como delito o falta sólo puede hacerse en atención a la pérdida de valor real de la cosa derivada de su menoscabo sustancial, porque la apelación al valor de uso supone confundir el daño a la cosa con el perjuicio, cuya presencia no resulta determinante para la configuración del delito. En este sentido, debe recordarse que para la integración de los daños no es preciso que se produzca un efectivo perjuicio en el patrimonio ajeno, bastando con que la cosa tenga valor económico, aunque su destrucción comporte un beneficio económico para el propietario. Prueba de ello es que el delito se castiga en función del daño causado, que debe ser superior a cincuenta mil pesetas (art. 263, 265, 267) (36). Como consecuencia, la cosa debe ser valorada objetivamente, quedando excluidos a efectos de cuantía los perjuicios y los daños morales.

Trasladando lo anterior a los daños en elementos lógicos se hace preciso, pues, que la conducta afecte a la estructura de los mismos, teniendo presente que aquí la cosa cuya sustancia debe verse afectada son los datos, los programas o los documentos electrónicos («... dañe los datos»). No, por tanto, el soporte magnético, físico, en el que se contienen los datos, cuya sustancia puede permanecer inalterada aún después de la destrucción de los mismos, ni los elementos físicos de la red o del sistema informático (hardware), sino los elementos lógicos (37). Y desde esta misma perspectiva debe darse contenido también a las modalidades de conducta.

Una interpretación literal estricta de esta conclusión podría llegar a entender que no son típicos por este art. 264.2 los daños que, dejando incólumes los datos -o afectándolos en términos insuficientes para integrar el delito, en los términos que a continuación se exponen-, determinan solamente una afectación del funcionamiento físico del sistema (haciéndolo más lento, provocando la aparición en pantalla de determinados dibujos o gráficos, ocupando la memoria o los soportes de almacenamiento con réplicas de rutinas que tienen la facultad de autocopiarse, etc.). Sin embargo, en la medida en que el funcionamiento del equipo se controla por programas (sistema operativo), tales alteraciones han de haber supuesto necesariamente una modificación de los mismos, por lo que la existencia o inexistencia del delito dependerá de que la afectación del programa pueda o no considerarse una destrucción, inutilización, alteración o daño del mismo (38).

Pero hay más. Al relacionar directamente la conducta constitutiva de daños con «los» datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos, el precepto parece estar haciendo referencia exclusiva a supuestos en los que la conducta se dirige directamente a la afectación de los mismos, pero no a aquéllos otros en los que se persigue dañar a los elementos físicos, aunque contengan datos. De ser así, como la destrucción de ciertos elementos físicos comportará necesariamente la destrucción de los datos, se produciría la paradoja de que cuando el sujeto lo que pretende es destruir directamente el equipo informático y no los datos, aún produciéndose el mismo resultado, debería apreciarse el tipo básico de daños del art. 263, mientras que si con la destrucción se trataba de dañar a los datos, habría de apreciarse el tipo agravado del art. 264.2. Para evitar tal consecuencia se hace obligado entender que están comprendidos en este tipo también los casos en los que la destrucción de los datos se produce mediante la destrucción del elemento físico que los contiene, y no sólo aquéllos en los que lo afectado son única y exclusivamente los elementos lógicos. Las referencias a «por cualquier medio» o «de cualquier otro modo», además de la lógica, recomiendan, pues, una interpretación de este tipo. Aunque debe añadirse que en estos supuestos la cuantía a tomar en cuenta será la del elemento físico y la de los datos dañados (39).

De acuerdo con estas precisiones deben ser interpretados las modalidades de conducta. Lo que tiene particular interés porque hay algunas formas de destrucción de ficheros mediante mandatos informáticos (delete, erase, borrar archivo, etc.) que no necesariamente suponen la desaparición física del mismo, sino que lo que generalmente provocan es su desaparición de los archivos ocultos de direcciones que permiten la identificación del mismo por el ordenador, impidiendo dar información al usuario de su existencia. Sin embargo, aunque el nombre del fichero borrado no aparezca en los listados de archivos existentes que proporciona el ordenador cuando se le solicitan mediante la orden correspondiente, el fichero -salvo que faltara espacio en el soporte físico y haya sido reemplazado por otro- sigue ahí. De hecho, la posibilidad de recuperar íntegramente ficheros borrados de esta forma es muy simple, bastando con utilizar mandatos (unerase, undelete, etc.) específicos para ello. Otro tanto sucede con los programas, cuya desaparición de la red, del soporte o del sistema informático no tiene porqué suponer necesariamente la pérdida del mismo, sino, simplemente, obligar a una nueva instalación.

Siendo así, la destrucción capaz de integrar el delito del art. 264.2 debe entenderse como desaparición completa y definitiva de los datos, programas o documentos (por cualquier forma: destrucción del soporte, interferencias magnéticas, eliminación de enlaces, pérdida de interpretabilidad por haberlos encriptado, etc.), en el sentido de que no es posible la recuperación íntegra de los mismos. Del mismo modo, la alteración, cualquiera que sea su forma (añadiendo nuevos datos, borrando parcialmente los existentes, eliminando o modificando las relaciones entre ellos, etc.) debe suponer una perturbación funcional definitiva, en el sentido de que los datos afectados acaban teniendo un contenido distinto al original (40). La inutilización resulta equivalente a la desaparición de su capacidad funcional, como puede ocurrir, por ejemplo, cuando se les protege con una clave de acceso desconocida para el titular. La simple ocultación del fichero no debe dar

lugar al delito, salvo que lo convierta en irrecuperable. Siendo así, podría ser una forma de dañar los datos «por cualquier otro modo».
Lo mismo puede decirse cuando no se borra fichero alguno, sino que se añade otro que, aún no afectando a los demás elementos lógicos incide en el funcionamiento del sistema, porque habrá afectado, como mínimo, al conjunto de programas que conforman el sistema operativo. En definitiva: la destrucción, la alteración, la inutilización o el daño han de comportar la alteración definitiva de la integridad de los datos, haciendo imposible su utilización o restauración tal y como estaban antes de la realización de la conducta (41).

Como consecuencia, deberá apreciarse la tentativa tanto cuando el virus, la bomba lógica o el procedimiento utilizado para causar los daños no llega a activarse (42), como cuando existan copias de respaldo o copias de seguridad de los ficheros o de los datos dañados, lo que hace que éstos puedan ser reincorporados al sistema o a la red sin especiales dificultades (43) o existen otras copias del programa que permiten su reinstalación. Y ello porque a pesar de que el sujeto ha realizado todos los actos de ejecución que deberían haber causado el resultado (la destrucción o pérdida de los datos, el programa o los documentos electrónicos), ésta no se produjo. El delito será consumado, en cambio, cuando aún habiendo copia de seguridad, éstas no sean idénticas. La cuantía a tomar en cuenta será la del elemento lógico dañado, integrándose en la responsabilidad civil los perjuicios que se deriven de la diferencia de valor entre el fichero destruido y el últimamente salvado.

2. Acceso ilícito a sistemas informáticos

El hacking es la denominación genérica con la que se hace referencia al acceso no autorizado a sistemas informáticos ajenos utilizando las redes públicas de telefonía o transmisión de datos (44). El éxito del mismo presupone que se han burlando las medidas de seguridad (contraseñas, claves de acceso, etc.) dispuestas para impedirlo y que ponen de manifiesto la voluntad del titular de que sólo las personas autorizadas por él puedan utilizar los recursos o ficheros informáticos o tengan acceso a la información que se contiene en los mismos. Las finalidades con las que puede realizarse el mismo son muy variadas. Desde descubrir secretos o datos reservados de otro o secretos de empresa (espionaje informático industrial), hasta la causación de daños o la ordenación de pagos o transferencias electrónicas de fondos, pasando por el que tiene móviles políticos o terroristas o persigue el apoderamiento de documentos electrónicos o programas de gran valor económico.

La preocupación por su desarrollo explica que haya sido objeto de tipificación expresa en algunos ordenamientos (45). No ocurre así en el Código penal español, que no contiene ninguna previsión que castigue de manera genérica el acceso no autorizado a sistemas informáticos ajenos. Como consecuencia, la punición de estos comportamientos sólo será posible en la medida en que vayan referidos a datos que sean objeto de protección particular o impliquen conductas que resulten incluibles en tipos penales genéricos.

De todos los supuestos posibles, en lo que sigue trataremos aquí dos: los accesos a sistemas, a ordenadores o a elementos lógicos ajenos en los que se contienen secretos de empresa (46) y el acceso que tiene por finalidad "apoderarse" de elementos lógicos de valor económico. Los casos en los que el acceso ilícito se realiza para llevar a cabo un perjuicio patrimonial ajeno (estafa informática) se tratarán dentro de los delitos producidos por medio del sistema informático (vid. supra III). Aquéllos que supongan la utilización ilegítima de terminales de comunicación (art. 256), que puede ser una modalidad delictiva apta para castigar determinadas formas de acceso ilegítimo a sistemas informáticos ajenos, se tratarán también de forma autónoma (vid. supra II.4). En todo caso, en la medida en que el acceso resulte punible en sí, las figuras eventualmente aplicables podrán concurrir en concurso de delitos con las que sancionen otros resultados punibles causados con el mismo (daños y descubrimiento de un secreto de empresa, estafa informática y utilización ilegítima de un terminal de comunicación, etc.).

A. ACCESOS ILÍCITOS A DATOS CALIFICABLES DE «SECRETOS DE EMPRESA»

Los «secretos de empresa» son objeto de protección en el art. 278.1, que constituye la referencia básica de estos comportamientos: «El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197» (prisión de dos a cuatro años y multa de doce a veinticuatro meses) (47).

El precepto se refiere expresamente a «datos, documentos ... electrónicos, soportes informáticos ...» (48), y por la remisión al 197 a «mensajes de correo electrónico ... telecomunicaciones ... o ... cualquier otra señal de comunicación», lo que lo sitúa de lleno dentro de los supuestos que tratamos en la medida en que el "apoderamiento" de los mismos supone de suyo un acceso no autorizado al sistema o al ordenador en el que los mismos se encuentran.

Para que la protección opere es preciso que en ellos se contenga un «secreto de empresa». Por tal se entiende toda información relativa a la industria o empresa que conocen un número reducido de personas y que por su importancia el titular desea mantener oculta. Comprende tanto los relativos a aspectos industriales (procedimientos de fabricación, investigación de nuevos productos o procedimientos, etc.) como comerciales (listas de clientes, tarifas y descuentos, distribuidores, estrategias comerciales, proyectos de expansión, etc.) y en general los relativos a la organización interna de la empresa cuyo conocimiento pueda afectar a su capacidad para competir (situación financiera, inversiones, relaciones con accionistas, etc.). Se comprenden tanto los que son fruto de las actividades de la propia empresa, su dueño, directivos o empleados, como los procedentes de tercero, que los ha cedido a título oneroso o gratuito.

La conducta que se castiga es doble. Puede consistir tanto en apoderarse por cualquier medio de los datos, de los documentos electrónicos o de los soportes informáticos en los que se encuentra el secreto, o en utilizar los medios del art. 197.1, en donde de nuevo se alude al apoderamiento de elementos lógicos («mensajes de correo electrónico») y a la interceptación de comunicaciones o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación. Sujeto activo puede ser cualquiera; sujeto pasivo es el titular de la empresa, cuya capacidad competitiva se ve afectada con la conducta, y que puede ser distinto del propietario de los papeles o datos de los que se apodera el autor.

Desde la perspectiva que ahora nos ocupa, referida a los elementos lógicos señalados, debe precisarse qué conductas pueden dar lugar al "apoderarse" que requiere el tipo. Como los «soportes informáticos» son elementos físicos -y su apoderamiento, por tanto, no plantea dificultad alguna- es evidente que la referencia a los datos, documentos electrónicos y mensajes de correo electrónico está hecha en la medida en que no se encuentran recogidos en soportes físicos, sino que están directamente en el sistema (en memoria RAM, por ejemplo) o, aún grabados en un fichero, su "apoderamiento" se produce directamente, sin tomar el elemento del hardware en el que se encuentra el archivo, sino actuando directamente sobre el mismo (49). En estos casos, las únicas formas posibles de realizar la conducta serían ver los datos directamente por pantalla, copiarlos en un soporte propio (con o sin destrucción del original) o transmitirlos a otro equipo informático o a una red.

Aunque en sentido propio "apoderarse" es tomar, coger, aprehender una cosa, ninguna dificultad se ofrece, sin embargo, para entender que estos comportamientos quedan comprendidos dentro del término (50). De una parte, porque el vocablo también tiene el sentido genérico de hacerse uno dueño de una cosa. Pero, sobre todo, porque tanto en este art. 278.1 como en el 197.1, el apoderamiento ha de efectuarse con la concreta finalidad de descubrir el secreto, lo que pone de manifiesto que lo determinante no es tomar para apropiarse, sino acceder al contenido del fichero y conocerlo. En definitiva: hacerse dueño del secreto. Como consecuencia, no hay dificultad para considerar típicos los casos en que el sujeto se limita a ver por pantalla el documento o fichero en el que se encuentra el secreto de empresa, sin tomar materialmente nada. Tanto la referencia a «apoderare por cualquier medio» como la inclusión de los supuestos del art. 197.1, de interferencia de telecomunicaciones o utilización de artificios técnicos de escucha y similares, muestra que basta la captación intelectual del secreto, aunque no se coja efectivamente nada. Así lo corrobora, igualmente, el apartado 3 del artículo -que después comentaremos detenidamente- y que advierte que el apoderamiento de los elementos en donde se encuentra el secreto «se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos». Con lo que se evidencia que el injusto propio del apartado 1 no comprende el implícito al tomar la cosa, sino que la referencia tiene un sentido instrumental en la medida en que deber ser el medio a través del que se accede al secreto de empresa. En todo caso, el término "apoderarse" lleva implícita la voluntad contraria del titular y la adopción por éste de medidas destinadas a mantener la reserva, lo que en el caso de elementos informáticos supone el establecimiento de códigos de acceso, palabras clave, contraseñas, etc.

Las conductas castigadas están sometidas, sin embargo, a muy concretas limitaciones. La primera, que el secreto se descubra como consecuencia de un apoderamiento o una interceptación, por lo que si

se llega al conocimiento del mismo por un camino distinto (por un error de dirección de quien envía el mensaje de correo electrónico, por ejemplo) no será posible apreciar el delito. Del mismo modo, el apoderamiento ha de hacerse «para descubrir un secreto de empresa», elemento subjetivo del injusto que sólo hace típicos los apoderamientos, la utilización de medios técnicos o las interceptaciones que se produzcan con esa finalidad.
«Descubrir» es conocer una cosa que se ignoraba, aunque no se haga partícipe a otros de ello. La consumación se produce, sin embargo, con el simple hecho del apoderamiento de los objetos o soportes en donde se contiene el secreto de empresa, o con la utilización de los medios técnicos, aunque el sujeto no llegue a saber o a conocer realmente el contenido del mismo. De hecho, por la naturaleza de su contenido no será inusual que quien realiza la conducta no esté en condiciones de captar su auténtico significado. Se trata de un delito de consumación anticipada en el que ésta se adelanta al momento mismo en el que el sujeto realiza la acción animado con el propósito típicamente requerido. A pesar de que no se exige expresamente perjuicio alguno, su causación va implícita en el propio concepto de secreto y en su relación con el bien jurídico protegido. En realidad, el simple conocimiento del mismo por personas ajenas a la empresa ya perjudica la capacidad competitiva de la misma.

En el apartado 3 del art. 278 se establece que «Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.» La previsión resulta sorprendente por partida doble. De una parte, porque lo que literalmente dice es que el posible concurso de delitos se apreciará sólo en relación con los soportes informáticos, pero no cuando se tratara de otros elementos (papeles, documentos escritos, medios audiovisuales, etc.); aunque tengan valor económico. De otra, porque al aludir a soportes informáticos, en rigor está comprendiendo sólo los casos en los que hay apoderamiento o destrucción del dispositivo físico en el que se encuentra grabado o recogido el secreto de empresa, con exclusión de aquéllos otros en los que el autor se limita a destruir o a copiar el elemento lógico en sí (borrado del fichero, eliminación de los datos en memoria volátil, por ejemplo).

A pesar de ello, debe entenderse que la posibilidad de concurso cabe en relación con cualquier elemento que contenga el secreto de empresa; siempre que tengan valor económico propio. Naturalmente, cuando la destrucción de los datos, del documento informático o del mensaje de correo electrónico pueda integrar el delito de daños (vid. supra II.1) o alguna de las figuras que se estudian a continuación.

B. APODERAMIENTO DE FICHEROS CON INFORMACIÓN DE VALOR ECONÓMICO NO CALIFICABLE DE SECRETO DE EMPRESA

Las anteriores figuras delictivas no resultan aplicables cuando la información contenida en los sistemas informáticos, redes o ficheros no puede ser considerada «secreto de empresa». Hay, sin embargo datos, documentos electrónicos y elementos lógicos no calificables de esa forma, pero de gran valor económico (estudios generales de mercado realizados con datos de dominio público, listados para envíos postales, costosas operaciones de procesamiento de datos, etc.) y que pueden ser objeto de comportamientos semejantes a los que, si se realizaran con elementos físicos, integrarían sin dificultad alguna delitos patrimoniales.

Así, junto a la destrucción de los ficheros -que dará lugar al delito de daños, en los términos ya examinados-, puede producirse la copia y el correlativo borrado del archivo del sistema informático en el que se encontraba, lo que resulta equivalente a la "sustracción" o al "apoderamiento" característico del delito de hurto. Igualmente, pueden obtenerse reproducciones no autorizadas del fichero, en términos parecidos a los que dan lugar a las defraudaciones de la propiedad intelectual. Obsérvese que, si en estos mismos casos, el sujeto se apodera o reproduce una copia de los datos o del fichero que el titular tiene en algún soporte físico (disco, CD-rom, reproducción impresa, cinta magnética, etc.) no se dudaría de la aplicación de esas figuras delictivas; pero ¿pueden ser invocables también cuando se trata de comportamientos que afectan directa y exclusivamente al elemento lógico en sí? (51). Veamos.

a) Eventual aplicación del hurto al "apoderamiento" de elementos lógicos

Como acaba de verse, tanto el art. 278.1 como el 197.1 utilizan el término "apoderarse" en relación con datos, documentos electrónicos y ficheros informáticos, reconociendo, por tanto, al menos en

principio, que, penalmente hablando, podría entenderse que tales elementos pueden ser objeto de sustracción (52). Desde esta perspectiva, por tanto, y concurriendo los demás elementos del hurto (ánimo de lucro, ajenidad de la cosa, valor económico), no habría dificultad alguna que impidiera la aplicación del delito.

La gran diferencia, sin embargo, viene dada porque en el hurto (y en el robo) se requiere una «cosa mueble» y hay dudas más que razonables de que los elementos lógicos pueden ser calificados de esta forma.

En sentido jurídico, cosa es todo elemento con valor económico determinado o determinable que puede ser objeto de derechos patrimoniales. Este concepto varía del naturalista y del civil (53) y ni siquiera resulta válido para todos los delitos patrimoniales (54). En las figuras de apoderamiento, puesto que se trata de "tomar", una de las características necesarias del objeto material ha de ser su aprehensibilidad, en el sentido de que puede ser cogida directamente, de manera que se requiere que la cosa tenga una individuación suficiente que permita su traslado de un lugar a otro (55).

Además, las cosas capaces de integrar el objeto material del delito de hurto han de ser susceptibles de apropiación, quedando excluidas por esta vía aquéllas que natural o jurídicamente no puedan fundamentar un derecho real de propiedad (las cosas communes omnium: la luz, el aire, etc.). Como consecuencia, la «cosa» que requiere el hurto (y el robo) podría definirse como todo objeto directamente aprehensible, susceptible de fundamentar un derecho patrimonial y valuable en dinero.

Junto a ello, ha de ser «mueble», categoría cuya noción es indiscutida y que desde una perspectiva funcional, viene entendiéndose como aquella que puede ser movilizada, que resulta trasladable; es decir, separada fácticamente del patrimonio de una persona e incorporada al del agente.

Concretado así el concepto de «cosa mueble» que precisa el hurto (y el robo), ¿lo son los datos, los documentos electrónicos y los ficheros informáticos en general? A mi juicio no. Aunque su capacidad para tener valor económico está fuera de toda duda, materialmente los elementos lógicos no son sino un conjunto de datos, informaciones o instrucciones que se recogen en un medio al que se accede eléctricamente. Unas veces, se encuentran en la memoria central del ordenador, a la que se llevan los programas o ficheros para procesarlos; otras, en dispositivos auxiliares de almacenamiento en los que se graba magnéticamente el programa o el fichero con vistas a su utilización futura (56). En este sentido, los elementos lógicos pueden ser considerados como una especie de flujo electromagnético, semejante a la energía eléctrica y demás energías, cuya calificación como «cosa mueble», al margen de la discusión doctrinal (57), fue resuelta inequívocamente en el derecho español en el sentido de no considerarla susceptible de integrar el objeto material que necesita el delito de hurto (y el robo).

En efecto, sin entrar ahora detenidamente en la cuestión, baste decir que la incorporación de las defraudaciones de fluido eléctrico y análogas, ya en el Código anterior, significa tomar partido a favor de quienes le niegan capacidad para integrar los delitos de apoderamiento. A partir de la ley de 10 de enero de 1941, que pasaría luego al Código de 1944, nuestro derecho positivo acogió la tesis partidaria de la necesidad de contemplación penal específica de la energía eléctrica, por lo que al recogerla expresamente el legislador optó por no considerarla una cosa susceptible de integrar la cosa mueble que requiere el hurto. De hecho, la incorporación de las defraudaciones de energía eléctrica y análogas acabó -como no podía ser menos- con la tendencia jurisprudencial partidaria de la aplicación del delito de hurto.

Por añadidura, los datos, los documentos electrónicos, los ficheros, los programas y la información que contienen se caracterizaban precisamente, como se vio (58), por no ser directamente perceptibles por los sentidos, lo que, cuando menos, descarta que sea una cosa aprehensible, haciendo que la polémica en torno a su conceptuación como material o inmaterial, corporal o incorporal, sea, a estos efectos, de escasa relevancia. Lo cierto es que, en cuanto flujo electromagnético, y a tenor del actual tratamiento legal dado a la energía eléctrica, no puede ser objeto material del delito de hurto (o robo), por ser materia de una tipicidad específica que parte de la base de su inidoneidad para ser considerada «cosa mueble», en el sentido de este delito. Por eso, dado que su naturaleza es la misma, tampoco los elementos lógicos de un sistema informático pueden merecer esa calificación, de manera que su apoderamiento no puede ser incluido, a mi juicio, dentro de las aludidas modalidades delictivas (59).

En el nuevo Código, por tanto, sigue siendo atípicos por hurto (o robo) los casos de copia fraudulenta de los elementos lógicos del sistema, equiparables por su dinámica comisiva y resultados prácticos al apoderamiento característico de estos delitos. Tan sólo cuando la copia vaya acompañada de la destrucción del fichero original podrá aplicarse el delito de daños, en los términos que han

quedado expuestos.

b) Aplicación de otras figuras delictivas

Para sancionar estas conductas, tampoco pueden aplicarse las defraudaciones de energía eléctrica y análogas. De una parte, porque no concurren los elementos precisos (suministro por aparatos contadores). De otra, y principalmente, porque en estos casos el flujo energético en su significación física no es el objeto de la defraudación, sino el vehículo de la misma. Lo importante no es el consumo ilícito de energía, sino la importancia económica de los datos: la cosa son los datos. Tampoco la utilización ilegítima de terminales de telecomunicación, como veremos, puede acoger supuestos de esta naturaleza.

La aplicación de la estafa, aunque no encuentra dificultades desde el punto de vista del objeto material (dado que no se requiere que sea cosa, bastando la realización de un acto de disposición del que se deriva un perjuicio patrimonial), se ve obstaculizada por la exigencia de engaño en unos supuestos en los que no hay ninguna conducta calificable de artificiosa. Si lo hubiera, como cuando se engaña al propietario o al encargado del sistema para que proporcione una copia del elemento lógico, la apreciación del delito no ofrece problemas. En todo caso, nunca puede hablarse de engaño en relación con el sistema informático, puesto que el destinatario del mismo ha de ser necesariamente una persona. Del mismo modo, la aplicación de la apropiación indebida, además de los problemas derivados del objeto material ya examinados para el hurto, encuentra los que ofrece el intento de delimitar lo que sería una atípica apropiación indebida de uso y la genuina apropiación requerida por el tipo.

Otro tanto sucede con los arts. 270 o 271, relativos a la propiedad intelectual, cuya virtualidad para castigar los apoderamientos por medios informáticos de elementos lógicos es muy limitada. Fundamentalmente porque en el art. 270 se tutelan directamente los aspectos patrimoniales relacionados con el derecho de autor, por tanto desde la perspectiva de la creación intelectual, mientras que los comportamientos que nos ocupan afectan al derecho de propiedad sobre el elemento material en el que se plasma la obra (corpus mechanicum), que corresponde a quien adquiere el objeto (60). La declaración del art. 3 de la Ley de Propiedad Intelectual (LPI) de que «los derechos de autor son independientes, compatibles y acumulables con la propiedad y otros derechos que tengan por objeto la cosa material a la que está incorporada la creación intelectual», a la par que resalta el diverso plano en el que se sitúa la protección en un caso y otro, pone claramente de relieve que no se contemplan en los arts. 270 y 271 los atentados a derechos que tienen por soporte al objeto material en el que se encuentra la obra, que son precisamente los que tienen relevancia desde el punto de vista que aquí nos ocupa de "apoderamiento" de elementos lógicos.

De hecho, si el presupuesto de la reproducción, el plagio, la distribución o la comunicación pública de una obra literaria, artística o científica fuera el apoderamiento de un ejemplar de la misma, debería darse lugar al correspondiente concurso de delitos. Lo que muestra la inutilidad de estos delitos para comprender los casos que tratamos. Ni siquiera bajo la forma típica de la «reproducción» podría acogerse la copia ilícita de un fichero -susceptible de integrar el objeto material de los delitos relativos a la propiedad intelectual- de valor económico hecha por quien accede ilícitamente al sistema. Y es que aunque la misma supone la fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella, la reproducción tiene un sentido que la conecta con un ámbito superior al del usuario individual. Ello se vería confirmado por la exigencia de que las conductas se produzcan «en perjuicio», lo que sugiere que sólo son típicas las reproducciones que van orientadas al público en general, con exclusión de las que se produzcan para mero uso privado por la misma persona que la lleva a cabo (61).

3. Protección penal de los programas de ordenador (62)

Al hablar de protección penal de los programas de ordenador interesa tratar fundamentalmente dos cosas: en primer lugar, en qué casos incurre en responsabilidad criminal quien reproduce y/o distribuye copias fraudulentas de los mismos (la conocida piratería); en segundo lugar, si comete algún delito el que adquiere o recibe las mismas. Además, nos ocuparemos de la nueva figura creada por el Código de 1995, de fabricación, puesta en circulación y tenencia de dispositivos o medios específicamente destinados a desproteger programas de ordenador (art. 270.2) (63).

A. PIRATERÍA DE PROGRAMAS DE ORDENADOR

a) Elementos de la conducta típica

En el derecho español la protección penal del software se articula a través de la que se presta a la propiedad intelectual (64), y, por tanto, mediante los artículos 270 y 271 del Código penal, cuyas previsiones deben ser interpretadas a tenor de lo dispuesto en el Título VII del Libro I del texto refundido de la LPI, artículos 95 a 10465. En lo que no esté expresamente previsto en el mismo serán de aplicación las disposiciones de la LPI. que resulten pertinentes (art. 95 LPI.).

De acuerdo con lo dispuesto en la LPI. (art. 10), ha de tratarse de creaciones originales, «expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro» (66). La referencia legal a obra literaria, artística o científica es un elemento normativo de valoración legal, para cuya concreción hay que acudir a lo dispuesto en la LPI. (art. 10).

Por programa de ordenador se entiende «toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación» (art. 96.1 LPI.). En cuanto tales son expresamente mencionados dentro de la enumeración de obras a las que se extiende la protección de la LPI. (art. 10.1 i), cualquiera que sea su forma de expresión (art. 96.3 LPI.) (67). La única condición para que un programa de ordenador pueda ser obra protegida es que sea original, en el sentido de resultar una creación intelectual propia de su autor (art. 96.2 LPI); o lo que es lo mismo: que sea fruto del esfuerzo intelectual del autor, y que, por tanto, no constituye una copia. Definidos en estos términos, los programas de ordenador entran de lleno en la protección que a las obras literarias dispensan los arts. 270 y 271 del Código penal.

La tutela penal comprende tanto al programa fuente como al programa objeto, a la documentación preparatoria (art. 96.1, párr. 2.º, que se considera parte integrante del programa) y a la documentación técnica y los manuales de uso (art. 96.1, párr. 2.º, que gozarán de la misma protección que los programas). No alcanza, en cambio, a las ideas y a los principios básicos del programa, incluidos los que sirven de fundamento a sus interfaces (art. 96.4 LPI). Respecto de éstas, lo que se protege son las formas de "expresión" de esas ideas, delimitación entre "idea" y "expresión" que ofrece importantes dificultades para hacerse con claridad, pero que resulta decisiva para concretar los términos de la tutela y, en particular, la posibilidad de plagio. Excluidos de la protección quedan en todo caso los programas que hayan sido creados con el fin de ocasionar efectos nocivos a un sistema informático (virus; art. 96.3). También pueden ser objeto material del delito las transformaciones de los programas de ordenador, lo que permite incluir a las versiones sucesivas y a los programas derivados.

Las conductas castigadas son la reproducción, el plagio, la distribución, comunicación pública, importación, exportación o almacenamiento de copias ilícitas, en los términos que quedan expuestos en el apartado anterior y con las precisiones que se hacen a continuación.

En cuanto al plagio, debe advertirse que no necesariamente lo integran ni las versiones sucesivas del programa ni los programas derivados, que son también objeto específico de protección en favor de quien las realiza en los términos de la Ley (art. 96.3 y 100.4 LPI.) (68). Sobre la transformación, ha de recordarse que comprende la traducción, la adaptación o el arreglo del programa. Tales actos forman parte de los derechos de explotación exclusivos que corresponden al titular de los mismos, por lo que su realización ha de contar con su autorización [art. 99, párr. 1º b) LPI.] (69). Cuando así sea, quienes las lleven a efecto gozarán también de derechos protegidos sobre la transformación. Se exceptúa de la necesidad de autorización, sin embargo, la transformación, incluida la corrección de errores, cuando ello resulte necesario para la utilización del programa por el usuario legítimo, con arreglo a la finalidad propuesta (art. 100.1 LPI.) (70).

En lo relativo a la reproducción (71), importa precisar sobre todo su concepto y si son o no delito las copias que se producen en el ámbito doméstico (casos como los de instalación del programa por el usuario más veces de las autorizadas, instalación en otro ordenador, cesión gratuita de copias a otros usuarios que lo utilizarán también para tareas privadas, etc.), que son los supuestos más frecuentes de piratería.

A estos efectos, debe recordarse que dentro de los derechos exclusivos de explotación del programa que corresponden al autor o a quien los haya adquirido se comprende la cesión del derecho de uso, mediante la cual se autoriza a otro a utilizar el programa, conservando el cedente la propiedad del mismo (art. 99, párr. 2º LPI.). Salvo prueba en contrario, se presumirá que la cesión no es exclusiva,

pero si intransferible y para satisfacer únicamente las necesidades del usuario (art. 99, párr. 2º LPI) (72). Como consecuencia, la reproducción total o parcial de un programa de ordenador, incluso para uso personal, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria, necesitará de la autorización del autor o del titular de los derechos de explotación [art. 99, párr. 1º a) LPI.]. Más claramente aún: «Cuando la carga, presentación, ejecución, transmisión o almacenamiento de un programa necesiten tal reproducción deberá disponerse de autorización para ello, que otorgará el titular del derecho» [art. 99, párr. 1º a) LPI.].

La única excepción en la que no se precisa autorización es para la reproducción que resulta necesaria para la utilización del programa por parte del usuario legítimo, con arreglo a su finalidad propuesta (art. 100.1 LPI.). O lo que es lo mismo: no integra la reproducción penalmente sancionada la introducción del programa en memoria interna a los solos efectos de su utilización por el usuario, salvo que se hubiera pactado lo contrario. Tampoco, la copia de seguridad por parte de quien tiene derecho a utilizar el programa, cuya realización no podrá impedirse por contrato en cuanto resulte necesaria para dicha utilización (art. 100. 2 LPI.).

Fuera de estos casos, la copia, instalación o utilización de cualquier programa de ordenador sin consentimiento del titular del derecho entra dentro del concepto de reproducción sancionado en este precepto. Como consecuencia, en principio podría resultar constitutiva de delito la copia no autorizada, la cesión onerosa o gratuita a tercero, la instalación más allá de las posibilidades cubiertas por la licencia de uso, etc., incluso si todo ello se produce en el ámbito doméstico y para uso privado. De hecho, la LPI. considera expresamente estos supuestos como infracción de los derechos de autor (73).

b) Ánimo de lucro y perjuicio

Sin embargo, para que la reproducción -y las demás conductas castigadas- sea constitutiva de delito es preciso que se lleve a cabo con «ánimo de lucro y en perjuicio de tercero», exigencias que no recogía expresamente el Código anterior y de cuya concurrencia depende en último término la aparición del delito en los casos que comentamos.

La interpretación del ánimo de lucro no ofrece particularidad alguna, puesto que se trata de un elemento subjetivo del injusto semejante al que se exige en otros delitos patrimoniales y cuyo sentido doctrinal y jurisprudencial es claro: ánimo de lucro equivale al propósito de obtener con la conducta una ventaja patrimonial ilícita. En definitiva, lo que el Tribunal Supremo viene definiendo como todo beneficio, ventaja o utilidad patrimonial que pretende obtener el sujeto con la conducta para sí o para tercero, incluso las meramente lúdicas, contemplativas o de ulterior beneficencia (74). Entendido así, no parece que pueda dudarse de la concurrencia de este elemento subjetivo del injusto en quien lleva a cabo la copia o reproducción no autorizada de un programa de ordenador. Incluso en la copia que se hace gratuitamente a un tercero concurre el ánimo de lucro, puesto que la liberalidad comporta una disposición patrimonial.

Más complicada es, en cambio, la interpretación del «en perjuicio de tercero», elemento cuya naturaleza resulta confusa. El sentido del tipo y la referencia conjunta al lucro y al perjuicio, en todo caso, pone de manifiesto tres cosas. La primera, que son conceptos que deben interpretarse en términos patrimoniales y económicos. La segunda, que el tipo considera que ambas exigencias son compatibles y separables. Lo que es cierto, dado que el propósito de obtener un provecho económico con la conducta no necesariamente tiene porqué comportar la finalidad de perjudicar al sujeto pasivo. Es más: el ánimo de lucro puede coexistir con el fin de que el titular del derecho resulte beneficiado y no perjudicado. Por ejemplo: cuando un programa que no ha obtenido beneficio alguno en su versión original es ligeramente modificado por otro, sin consentimiento del autor, convirtiéndose en un éxito de ventas, cuyas ganancias comparten entre ambos; supuesto en el que hay ánimo de lucro, pero no ánimo de perjudicar. La tercera, que la acumulación de ambos pretende limitar el ámbito de aplicación del tipo, que resulta más restringido que cuando se requiere sólo uno u otro.

Partiendo de estas premisas, la expresión «en perjuicio» puede entenderse de alguna de estas tres formas: 1) como exigencia efectiva de que como consecuencia de la conducta se cause un perjuicio en el patrimonio ajeno, lo que lo convertiría en el resultado del delito; 2) como elemento subjetivo del injusto, que expresaría una finalidad específica en la conducta de necesaria concurrencia para que el hecho resulte típico; o 3) como una característica objetiva del comportamiento, en el sentido de que éste ha de resultar objetivamente idóneo (por el número de copias, por su precio, por la forma de

distribución, etc.) para causar un perjuicio ajeno, elemento que sólo haría típicos los que tuvieran esa capacidad potencial y que debería ser comprendido por el dolo del autor.

La consideración del perjuicio como resultado de la conducta puede verse corroborada por la redacción del tipo agravado del art. 271. b), que se refiere al «daño causado», lo que sugeriría que en el tipo básico ha debido necesariamente causarse alguno. Sin embargo, el perjuicio no tiene incidencia alguna en la determinación de la pena, lo que no se corresponde con la técnica usual seguida por el Código cuando lo concibe como resultado del delito (estafa, por ejemplo). Además, la falta del mismo determinaría que en los casos en los que no llegara a producirse debería apreciarse la tentativa, con lo que no se conseguiría el propósito de limitar la intervención penal.

La consideración como elemento subjetivo del injusto, en cambio, excluiría su aplicación en más casos de los deseables, porque lo común en supuestos de esta naturaleza no es tanto que se quiera perjudicar a otro, cuanto obtener un lucro para sí, por lo que exigir en el sujeto que la conducta tenga como una de sus finalidades causar un perjuicio ajeno, añadido al ánimo de lucro, determinaría la impunidad de muchos supuestos.

Por eso, a mi juicio, el «en perjuicio» debe interpretarse como una condición objetiva de la conducta, que, por las circunstancias en las que se produce, tiene la idoneidad suficiente para perjudicar a los titulares de los derechos de la propiedad intelectual, lo que constituye un elemento del tipo que debe ser comprendido por el dolo del autor. Ello significa, por ejemplo, que no serán típicas, por falta de ese capacidad potencial, las infracciones que se produzcan para mero uso privado por la misma persona que la lleva a cabo.

La conclusión se ve avalada, además, por la propia sistemática legal. Aún con una dimensión patrimonial inequívoca, los delitos relativos a la propiedad intelectual han sido alojados por el legislador dentro del ámbito de lo socioecómico, precisamente en el Título XI, dedicado a los delitos «relativos a la propiedad intelectual e industrial, al mercado y a los consumidores» (75). Como consecuencia, implícita en las conductas castigadas está la capacidad potencial de las mismas para incidir en el mercado, lo que supone excluir de la responsabilidad penal aquéllas que, por producirse en el ámbito estrictamente privado, no tengan esa potencialidad lesiva.

Como consecuencia, la copia no autorizada de un programa hecha por un usuario a otro, la instalación no permitida y comportamientos semejantes no son capaces de configurar el delito del art. 270 del Código penal.

B. ADQUISICIÓN O RECIBIMIENTO DE COPIAS NO AUTORIZADAS DE PROGRAMAS DE ORDENADOR

El art. 298 castiga como receptador al que «con ánimo de lucro y con conocimiento de la comisión de un delito contra el patrimonio o contra el orden socioeconómico en el que no haya intervenido ni como autor ni como cómplice, ayude a los responsables a aprovecharse de los efectos del mismo, o reciba, adquiera u oculte tales efectos». ¿Podrá servir este delito para castigar a quienes reciben copias no autorizadas de programas de ordenador, aunque sea para uso privado? (76).

De las dos modalidades de conducta que se recogen, la primera-ayudar a los responsables a aprovecharse de los efectos del delito-, se integrará sin dificultad siempre que concurran los elementos del delito. Más interesante, a los efectos que tratamos, es la que consiste en recibir, adquirir u ocultar, con ánimo de lucro, las reproducciones ilícitas de los programas (77).

La adquisición integra el delito tanto si es gratuita como si se produce mediante precio, cualquiera que sea éste; incluso si es muy superior al del mercado. La recepción parece referirse a la entrega gratuita de los efectos. La ocultación, equivale a esconderlos, aunque siguen siendo de quien los entregó. En definitiva, estas conductas integran el aprovechamiento propio que se ha considerado siempre característico de la receptación y en el se incluye cualquier beneficio, ventaja o utilidad patrimonial que obtenga o se proponga obtener el presunto receptador de los efectos del delito antecedente, incluso los meramente contemplativos, destructivos o de ulterior beneficencia o liberalidad.

Sujeto activo sólo puede serlo quienes no hayan intervenido ni como autores ni cómplices en el delito contra el patrimonio o contra el orden económico del que provienes los efectos, puesto que si fueran responsables del mismo las conductas que aquí se castigan aparecen como actos posteriores impunes perteneciente al agotamiento del delito previo. La referencia a los «autores» debe entenderse en el sentido amplio del art. 28, comprensiva de coautores, autores mediatos, inductores y

cooperadores necesarios.

El delito principal del que provienen los efectos ha de ser, por expresa exigencia legal, «contra el patrimonio o contra el orden socioeconómico», lo que coincide con la rúbrica del Título XIII. Entre ellos se incluyen los relativos a la propiedad intelectual, por lo que ninguna dificultad se ofrece en relación a este elemento. Los «efectos del delito» de los que se beneficia el sujeto son los que integran el objeto material del previo atentado patrimonial o socioeconómico; en esta caso, las copias ilícitas de los programas de ordenador.

El «conocimiento de la comisión de un delito» de esta naturaleza, elemento del dolo, equivale a conocimiento de que la copia que se adquiere, recibe u oculta proviene de un delito, lo que, con alguna vacilación, viene interpretándose como certeza y no como simple sospecha. No es preciso, sin embargo, que el sujeto conozca ni la calificación jurídica exacta del delito previo ni las circunstancias concretas en que se produjo (78). Del mismo modo, para castigar al receptador no es necesario conocer a los autores y partícipes del delito del que provienen los efectos; ni siquiera se precisa que el delito principal haya sido castigado (79).

Puesto que el ánimo de lucro puede considerarse presente en quien recibe o adquiere una copia pirata de un programa (80), el dato determinante de que pueda o no apreciarse la receptación dependerá de que la realización de la misma integre un delito contra la propiedad intelectual. Cuando al sujeto le conste que la copia es fruto de una reproducción ilícita con incidencia en el mercado -que son las únicas que pueden integrar un delito contra la propiedad intelectual (81)-, su comportamiento podrá calificarse de receptación. En la mayor parte de los casos, tal conocimiento podrá darse por sentado en quien adquiere la copia en ciertas condiciones (a través de anuncios u ofertas dirigidas al público en general en condiciones de venta inferiores al valor del mismo, presentación de las copias -características del soporte, inexistencia de carátulas o imitaciones burdas, etc.-, falta de manuales o licencias de uso, etc.). El error vencible sobre el origen de la reproducción (por ejemplo: creencia de que se trata de un programa original en especiales condiciones de venta o de un producto de dominio público o shareware (82))provocará la exención de responsabilidad criminal por receptación, puesto que se tratará de un error de tipo y no está castigada la forma imprudente de comisión (art. 14.1). En todo caso, el error invencible sobre la procedencia de la copia será poco verosímil, dado que generalmente los usuarios tienen unos conocimientos informáticos mínimos que hacen poco aceptable la posibilidad del mismo. Otro tanto ocurre con la creencia de que no es ilícito adquirir copias piratas (error de prohibición). En cualquier caso, el error invencible -poco factible en la práctica- deberá eximir de responsabilidad criminal; el vencible, dará lugar a la imposición de la pena inferior en uno o dos grados (art. 14.3º).

La adquisición o recibimiento de una copia no autorizada de un programa procedente de un usuario particular, que no tiene virtualidad para integrar el «en perjuicio» que requiere el delito contra la propiedad intelectual, tampoco podrá dar lugar a la receptación. Sencillamente, porque no procederá de un delito contra el patrimonio o contra el orden socioeconómico. Y ello incluso si el sujeto la recibe creyendo lo contrario, supuesto en el que se produciría un "error al revés" o un delito putativo, que, a mi juicio, resulta impune en el derecho español (83).

C. CONDUCTAS RELACIONADAS CON LA DESPROTECCIÓN DE PROGRAMAS DE ORDENADOR

Como tipo complementario, el párrafo tercero del art. 270 dispone que «Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador» (84). Con esta previsión lo que se hace es considerar como delito la fabricación, puesta en circulación, incluso gratuita, o la tenencia de medios físicos o lógicos (copiones) específicamente dirigidos a desproteger programas de ordenador, con el fin de poder efectuar reproducciones, instalaciones o copias no autorizadas de los mismos. La exigencia de que el medio sirva «específicamente» para esa finalidad debe servir para limitar drásticamente la aplicación del precepto, que no sería invocable, por ejemplo, respecto de medios que, junto a la posibilidad de desproteger programas, incluyan utilidades distintas (compresión/descompresión de ficheros, encriptación/desencriptación, comparar, formateos especiales, etc.)

La conducta típica incluye la fabricación, puesta en circulación y tenencia de tales programas o dispositivos. No se requiere ni ánimo de lucro ni perjuicio de tercero, por lo que puede resultar

constitutiva de delito la mera tenencia de los mismos por cualquier usuario que los emplea exclusivamente para su uso privado. Interpretado en estos términos, el precepto viene a castigar simples actos preparatorios, lo que, sobre todo en relación con la mera tenencia, creo que lleva demasiado lejos la intervención penal; aunque muy probablemente lo que se pretendía era comprender precisamente estos supuestos. En realidad, aún sin desconocer las diferencias que median entre unos casos y otros, pueden hacerse a esta modalidad de conducta objeciones semejantes a las que en su día se dirigieron a la tenencia de útiles para el robo, que ha desaparecido en este Código (85). Por eso que crea que, aunque expresamente no se requieran, debe exigirse también el ánimo de lucro y el «en perjuicio» en este apartado 2; lo que servirá para limitar el contenido de la mera tenencia, pues es evidente que los mismos pueden considerarse implícitos tanto en la fabricación como en la puesta en circulación.

4. Utilización ilegítima de terminales de comunicación

La utilización ilegítima de equipos informáticos, que se usan sin autorización del titular de la instalación o para fines privados, distintos de los permitidos (confección de programas propios, gestión de tareas extrañas, acceso a redes, acceso a Internet, etc.), es un comportamiento frecuente en los centros de proceso de datos. El perjuicio económico que puede significar esta especie de hurto de "tiempo-máquina" puede ser muy alto, especialmente cuando se refieren a las comunicaciones o a instalaciones o programas en alquiler, cuyo canon se satisface por el titular según el tiempo de uso.

El tratamiento que haya de darse a este tipo de supuestos depende de la solución general que se adopte en torno al hurto de uso, consistente en la utilización de una cosa sin derecho alguno o para un uso distinto al autorizado y en el que lo lesionado no es directamente la propiedad, sino una de las facultades inherentes a la misma, marcándose la diferencia con el hurto propio y con la apropiación indebida en la ausencia de ánimo de apoderamiento de la cosa (86). Por esta razón, al limitar el Código anterior la punición de las modalidades de uso a los vehículos de motor, este tipo de hechos resultaba atípico (87).

El nuevo Código introduce novedades significativas en este campo mediante una doble modificación. De una parte, haciendo referencia expresa a las «telecomunicaciones» dentro de las defraudaciones de energía eléctrica y análogas (art. 255). De otra, incorporando un tipo específico, que sanciona expresamente la utilización ilegítima de equipos terminales de telecomunicación (art. 256).

La mención de las «telecomunicaciones» que hace ahora el art. 255 permite incluir las defraudaciones en el teléfono, la televisión por cable o de pago, la transmisión de datos -analógica o digital-, el acceso a bancos de datos, etc., siempre que tales servicios se suministran mediante redes o instalaciones distribuidoras y se tarifen mediante aparatos contadores o instrumentos específicos de recepción y fijación del consumo, cualquiera que sea su clase o configuración técnica. Lo que en el mismo se sanciona es, pues, el uso en beneficio propio y en perjuicio del suministrador de este tipo de energías o fluidos cuando ello se hace con comportamientos que afectan directamente a la red de distribución o prestación del servicio o a los mecanismos o verificaciones precisas para la determinación del consumo efectuado (88). No se comprenden, en cambio, los supuestos de utilización ilegítima de sistemas informáticos que funcionan con las energías o acceden a los servicios defraudados, que sólo resultan punibles en los términos del art. 256. En definitiva: en el art. 255 lo que se castigan son las defraudaciones realizadas por el titular del sistema informático (o por su orden) en perjuicio de quien le suministra el servicio, mientras que los casos genuinos de utilización ilegítima de equipos son las que se produce en perjuicio del propietario de los mismos por quienes están encargados de su manejo. Las «telecomunicaciones» defraudadas han de tener un valor superior a cincuenta mil pesetas; si fuera inferior se integrará la falta del art. 623.4.

Las defraudaciones que se producen como consecuencia de la indebida utilización de terminales de telecomunicación, sin consentimiento de su titular, cuando se causa un perjuicio superior a cincuenta mil pesetas se castigan en el art. 256 (pena de multa de tres a doce meses). Si el perjuicio fuera inferior a cincuenta mil pesetas, se integrará la falta del art. 623.4. El perjuicio puede producirse por cualquier concepto derivado del uso no autorizado: importe de la energía consumida, gasto telefónico que pueda haberse producido, costos de accesos a bases de datos, importe del alquiler de los equipos indebidamente empleados, etc. "Terminales de telecomunicación" son todos los que, cualquiera que sean sus características concretas, sirven para establecer conexiones a distancia entre personas,

sistemas o dispositivos técnicos, mediante procedimientos eléctricos, radioeléctricos, informáticos, telefónicos, etc. (teléfono, fax, videoconferencias, correo electrónico, etc.).

El uso no autorizado puede consistir tanto en la utilización del terminal ajeno sin consentimiento del dueño como en su empleo en tareas o con finalidades distintas de las permitidas. Además de estos casos, el precepto puede acoger determinadas formas de hacking, como el acceso ilícito mediante un ordenador propio a redes o sistemas informáticos ajenos, utilizando de esa forma recursos o programas instalados en el mismo.

Obsérvese que sólo se sanciona la utilización de equipos informáticos cuando éstos cumplen funciones de terminales de telecomunicación, pero no cuando sirven simplemente para el procesamiento de información de manera autónoma. Ni siquiera está incluida la indebida utilización de ordenadores conectados en una red local, unidos directamente entre sí e integrados en un conjunto de equipos de funcionamiento interdependiente. Cuando no haya esta dimensión externa, el hecho sólo podrá dar lugar a un ilícito civil (o laboral). La diferencia establecida entre unos casos y otros -que puede discutirse- resulta coherente con las recomendaciones de la intervención mínima, que tan ignoradas han sido en otros lugares del Código, y que posiblemente hubieran sido desbordadas si se hubiera hecho una punición general de todos los casos de utilización ilegítima de equipos informáticos (89).

III. ILÍCITOS PATRIMONIALES REALIZADOS POR MEDIO DEL SISTEMA INFORMÁTICO

Vistos los comportamientos en los que el sistema informático o sus elementos son el objeto material del delito, tratamos ahora los ilícitos patrimoniales que se realizan sirviéndose de uno u otros, que aparecen como instrumento necesario para la realización de la correspondiente conducta típica. La peculiaridad de estos hechos, denominados generalmente fraudes informáticos, viene dada, pues, no por el objeto material del delito, sino por su peculiar dinámica comisiva, en la que el sistema informático es el instrumento o el medio a través del que se produce el hecho lesivo del patrimonio ajeno. Como ya se advirtió, en muchos de los supuestos posibles concurrirá la doble dimensión expuesta de tratarse de comportamientos que se realizan contra elementos informáticos y por medio de procedimientos informáticos. Cuando así sea, el análisis deberá hacerse desde esa doble perspectiva. Ninguna referencia se hará, en cambio, a los casos en los que el sistema informático se utiliza para cometer delitos "tradicionales" en los que la utilización de estos medios no añade particularidad alguna respecto de los que se realizan por otros medios.

1. Estafa por medios informáticos

La informatización de las transacciones financieras, comerciales y bancarias, la generalización del pago a través de procedimientos electrónicos, el desarrollo de la gestión y de los procesos contables mediante sistemas de esta naturaleza, ha abierto formas inéditas de comisión a los delitos patrimoniales y económicos que hasta hace poco no han merecido ni doctrinal ni legalmente el interés que por su importancia merecían. Las redes de transmisión de datos, igualmente, facilitan aún más la posibilidad de delito, al permitir que el autor pueda efectuar las modificaciones desde su propio domicilio, si dispone de un terminal y un instrumento de transferencia de datos adecuado.

Las manipulaciones más usuales se producen normalmente mediante la introducción de datos falsos, la alteración de los programas o la utilización de bombas lógicas, caballos de Troya, el hacking, ya analizados (90), o técnicas como la del salami (91), que provocan la realización automática de transferencias bancarias, ingresos o reconocimiento de créditos en favor de quien realiza la alteración (92). El medio empleado y la actuación con y sobre máquinas y no sobre personas, junto con el hecho de que la conducta utilice e incida en elementos incorporales, son los caracteres definidores de estos supuestos y los que les dan identidad propia desde el punto de vista penal.

Hasta el Código de 1995 la mayor parte de estos hechos resultaban atípicos y muy en particular las transferencias electrónicas de fondos, que constituyen el núcleo central de los mismos (93). En efecto, la noción de cosa sobre la que se construyen los delitos de apoderamiento (94) hacía imposible la aplicación de tales figuras delictivas, dada la imposibilidad de considerar «cosa mueble» a la llamada moneda escritural o moneda de giro. Y es que lo que se crea como consecuencia de la falsa

introducción de datos, de los asientos, de las órdenes, instrucciones o transferencias fraudulentas, son derechos de crédito (una especie de "deuda de valor") en favor de la persona a la que se le reconocen (95). La transferencia bancaria no supone sino la realización de un asiento contable en virtud del cual se reconoce al titular de la cuenta corriente un derecho de crédito por el saldo resultante, por lo que entender que en estos casos estamos ante una «cosa mueble» significaría recurrir a la analogía prohibida (96).

Por razones semejantes, tampoco era posible considerar realizado un delito de apropiación indebida, dadas las grandes dificultades que ofrece el entender presente el título en virtud del cual se ha recibido la cosa o el activo patrimonial y del que surge la obligación de devolverla (97).

La aplicación de la estafa era, igualmente, inviable, aunque por razones distintas. Ninguna dificultad ofrecía el objeto material, que no tiene porqué ser necesariamente una cosa mueble. Por otra parte, frente al «tomar» del hurto, la estafa implica una dinámica comisiva más ideológica, que permite incluir dentro de ella transferencias de fondos, operaciones bancarias y créditos, que suponen un desplazamiento patrimonial, con independencia de la materialidad del traslado real. El inconveniente aquí era la concepción legal del engaño, limitado a aquéllos que se producen entre personas, únicas, por lo demás, respecto de las que tienen sentido las referencias al «error» y a la "inducción" del acto de disposición patrimonial. Por eso que se afirmara que cuando el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de disposición patrimonial, no se produce ni el engaño ni el error necesarios para la estafa (98).

Para salvar esta laguna de punición, y atendiendo a la demanda doctrinal de un tipo específico que contemplara estos casos (99), el apartado 2 del art. 248 establece que «También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la trasferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.» (100).

La referencia a «alguna manipulación informática o artificio semejante» es capaz de acoger todos los casos posibles mediante los que se efectúa una trasferencia no consentida de activos patrimoniales en perjuicio de tercero, ya consistan en modificaciones de programas o alteraciones en el procesamiento, ya en manipulaciones en la entrada, salida o transmisión de datos. Como se ha observado, la fórmula legal es muy amplia, aunque tal vez inevitable en este campo, en el que el desarrollo tecnológico es continuo, con el peligro de que una prosa más estricta dejara pronto obsoleto el precepto (101). La referencia a «artificio semejante» podría hacer pensar que se incluyen también otras maniobras de naturaleza no informática. Sin embargo, el sentido del apartado obliga a entender que todo él va referido a estos supuestos, por lo que la mención legal debe ser interpretada también desde esa perspectiva.

Con esta salvedad, los elementos del delito siguen siendo semejantes a los de la estafa. Se requiere ánimo de lucro; la manipulación informática o el artificio semejante, equivale al engaño bastante y al error; la transferencia no consentida es el acto de disposición que provoca el perjuicio para tercero, elemento que también se requiere. Igualmente, se precisa la relación causal entre la manipulación informática, la transferencia electrónica y el perjuicio ajeno (102). Debe tenerse presente que lo común será que la transferencia se haga directamente por el sistema informático que recibe la orden fraudulenta, por lo que la referencia a «no consentida» no puede entenderse como existencia de un acto concreto de voluntad contrario a la transferencia, que no existirá, sino como orden de cargo hecha en activos patrimoniales ajenos sin derecho a ello.

El precepto castiga únicamente las transferencias electrónicas de fondos, sin comprender las conductas que no provoquen una operación de este tipo. No son incluibles aquí, por tanto, sino en la modalidad delictiva que corresponda en cada caso, las manipulaciones que se dirijan a encubrir apoderamientos o disposiciones efectuadas por otros medios (por ejemplo: modificar inventarios para ocultar la sustracción de materiales, alterar la contabilidad para encubrir desfalcos, etc.).

Transferir es trasladar, cambiar de un lugar a otro. En el sentido del texto, ello constituye un proceso meramente contable que supone cargar débitos, descontar activos u ordenar ingresos con la correlativa anotación a favor de otro sujeto, al que se reconoce, de esta forma, un derecho de crédito o en favor del que se realiza una cierta prestación o servicio: billetes de transportes que se cargan a otros, ingresos ficticios en cuentas corrientes, abonos de salarios no debidos, cargos por materiales no suministrados, órdenes de pago falsas, etc. La consumación se alcanza cuando se produce el perjuicio, lo que coincidirá con la realización del asiento contable. Es posible la tentativa.

La determinación de la pena se hará, como en la estafa común, conforme al art. 249. Las agravaciones del art. 250 son también aplicables a esta modalidad de estafa, aunque algunas de ellas no son concebibles en relación con la misma (103).

2. Apoderamientos de dinero utilizando tarjetas de cajeros automáticos

El abuso de cajeros automáticos es otro de los comportamientos más frecuentes entre los ilícitos patrimoniales realizados por medio de sistemas informáticos (104). El instrumento que se utiliza para ello es la tarjeta de crédito que, como es sabido, puede cumplir la triple función de instrumento de pago, de garantía y de crédito, incluyendo en ésta última la obtención de dinero en metálico (105). Los casos que interesan tratar ahora son, sin embargo, aquéllos en los que cumple esta última función en cajeros automáticos, puesto que cuando se utiliza como instrumento de pago los problemas que se plantean son sustancialmente distintos.

En efecto, el uso indebido de tarjetas de crédito con esta finalidad debe ser analizado desde la perspectiva de la estafa, puesto que -de haberlo- el engaño se produce sobre «otro» y no directamente sobre el sistema informático. De hecho, la jurisprudencia ha venido apreciándola sin dificultad, entendiendo que el uso indebido de las mismas, a la que se cargan cantidades superiores al crédito disponible, supone una apariencia de solvencia frente a quienes se exhibe que no responde a la realidad de los fondos existentes (106).

Por el contrario, la utilización de la tarjeta para extraer dinero de un cajero es equiparable al de las maniobras físicas sobre máquinas automáticas (cabinas telefónicas, máquinas de tabaco, bebidas, etc.), cuando se persigue obtener de ellas el producto o el servicio sin la correspondiente contraprestación económica; casos que deben ser calificados como hurto cuando lo que se obtiene es una cosa mueble (107). Hay objeto material, dado que se obtiene dinero y no un asiento contable. La posibilidad de estafa debe ser descartada de antemano puesto que no hay engaño a «otro», como requiere el tipo básico del art. 248.1, ni se trata de una transferencia no consentida de activos patrimoniales, como precisa el 248.2, sino directamente de la obtención de dinero, que puede ser calificado de «cosa mueble» (108).

Como consecuencia, en principio, los casos de obtención de dinero de un cajero automático deben ser analizados desde la perspectiva del hurto; aunque, como veremos, una buena parte de las hipótesis posibles son atípicas, por faltar alguno de los elementos que requiere el mismo. Respecto de las que lo sean, deberá concretarse, además, si la utilización de la tarjeta es capaz de integrar el concepto de fuerza en las cosas y, por tanto, si, cuando concurran los demás elementos del delito, cabe la calificación de robo con fuerza en las cosas (109).

A. ABUSO DE CAJEROS AUTOMÁTICOS

Las extracciones que se producen por el titular de la tarjeta, tanto si se mantiene dentro del saldo disponible como si lo excede, son, a mi juicio, atípicas (110). En el primer caso, porque no hay apoderamiento de cosa ajena, puesto que se respeta el máximo de saldo disponible. Si las extracciones se producen en el mismo día es posible que sea preciso manipular la tarjeta -sobre todo en los sistemas off line, cada vez más raros-, en cuya banda magnética suele reflejarse la fecha y el máximo de la extracción diaria posible (111). La repercusión penal de ello debe analizarse desde la perspectiva de las falsedades, en los términos que a continuación se detallan.

Cuando lo que se producen son extracciones repetidas por el titular, hasta superar el saldo disponible, podría pensarse que hay, en principio, apoderamiento de una cosa mueble ajena. No obstante, falta también en estos casos la ajenidad del dinero recibido y la ausencia de consentimiento del propietario de la cosa, puesto que el contrato de depósito en cuenta corriente o de apertura de crédito que vincula a la entidad y al usuario de la tarjeta genera entre ellos recíprocos derechos de crédito y acepta la posibilidad de descubiertos; lo que podría considerarse un consentimiento tácito sobre la obtención de dinero por cuantía superior a la del depósito existente en el momento de realizar la extracción (112). Todo ello sin mencionar la posibilidad de que ello suponga un comportamiento atípico como consecuencia de la aceptación del riesgo que supone la delegación en el usuario de funciones de autoprotección que corresponden a la entidad emisora (113). Como antes, la manipulación de la tarjeta que pueda resultar precisa deberá ser analizada desde la perspectiva de las falsedades, que comentamos después.

Cuando el titular utiliza una tarjeta anulada o caducada, estamos ante un caso de utilización de la

tarjeta por un tercero sin derecho a ello. Al no haber ningún contrato vigente entre entidad bancaria y titular, no hay dificultad en apreciar directamente un hurto por la cantidad que se obtenga (114). La retención de la tarjeta por el cajero, al percibir la anomalía, dará lugar a la tentativa.

Distinto es el tratamiento que merecen los casos en los que la extracción de dinero se produce por un tercero con tarjeta falsificada, perdida o sustraída al titular. Si la tarjeta fue encontrada y no devuelta se integraría una apropiación indebida; si fue sustraída, un hurto, y si se obtuvo mediante engaño, una estafa; en los tres casos, por el importe de la tarjeta en sí, lo que significará apreciar una falta (115). Sujeto pasivo de estas infracciones será el propietario de la tarjeta, que normalmente es la entidad emisora. A menudo, como se la quiere para usarla y devolverla después, lo que se realizaría serían esas infracciones en su modalidad de uso que, como es sabido, son atípicas. La obtención del número de identificación personal mediante engaño no integra la estafa respecto de lo que después se obtiene del cajero con la tarjeta. Y es que en estos casos, en los que se "engaña" a un cajero, la figura aplicable es el hurto y no la estafa (116). Respecto del dinero que se extraiga el apoderamiento de la tarjeta no es un acto de ejecución, por lo que la sustracción sólo será punible en cuanto tal, sin integrar ya, además, la tentativa de robo (117).

El dinero que se obtiene del cajero automático con la tarjeta ajena, dará lugar a un hurto -salvo lo que se diga respecto de la fuerza en las cosas-. La concreción de quién es sujeto pasivo y quién perjudicado dependerá de las cláusulas contractuales que se hayan establecido en los casos de pérdida o sustracción y las obligaciones y responsabilidades que asuman el titular, por una parte, y la entidad emisora, por otra. (118). La simple utilización de la tarjeta supone ya la realización de actos de ejecución, por lo que, si por causas ajenas a la voluntad del sujeto, el dinero no llegara a obtenerse, se apreciará la tentativa (119). De ser punible la apropiación de la tarjeta, se dará lugar al correspondiente concurso medial (ideal) de delitos. La falsificación de la misma podrá concurrir también en los términos que después se tratan.

B. UTILIZACIÓN DE TARJETAS DE CAJEROS AUTOMÁTICOS Y FUERZA EN LAS COSAS

Por expresa disposición legal, tienen la consideración de llaves «las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia» (art. 239, párr. 2º); elementos, por otra parte, que ya venía tratando como tales tanto doctrina como jurisprudencia (120). Como consecuencia, la utilización de una tarjeta para abrir el habitáculo en el que se encuentra un cajero automático podrá integrar este supuesto si es falsa (121). Esta consideración tienen, en todo caso, las «legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.» (art. 239.2º) (122).

Puede dudarse, sin embargo, de que la solución sea la misma si la tarjeta se utiliza para obtener directamente el dinero del cajero, puesto que aquí no puede decirse que sirva para abrir un cierre, sino que desencadena un proceso mecánico en virtud del cual se produce la entrega automática del dinero, por lo que no cumple realmente la función de llave. Por esta razón, mientras que un sector doctrinal dudaba que en estos casos pudiera apreciarse el robo (123), otro, en cambio, no encontró dificultades para estimarlo (124).

La mención expresa que ahora se hace a todo tipo de tarjetas es lógico pensar que ha debido incluirse con la finalidad de comprender también estos casos dentro del robo; no obstante, considero que si la tarjeta no abre nada, no puede hablarse de uso de llaves falsas. Y es que consubstancial al concepto de llaves es ser un instrumento destinado a abrir una cerradura, como reconoce el Código al equiparar a las mismas a las ganzúas y, expresamente, al considerar como tales cualesquiera otras que no sean las destinadas por el propietario «para abrir la cerradura violentada por el reo» (art. 239.3º). Con ello no se hace sino aplicar a las tarjetas -y a los cajeros automáticos- el mismo tratamiento que se viene dando a casos similares, en los que se niega el robo cuando la llave sirve para otra función distinta de la de abrir (por ejemplo: arrancar un coche, activar el alumbrado, etc.).

El problema no es, pues, que una tarjeta magnética no pueda ser una lleva, que puede serlo, como reconoce el propio Código, sino que es tal sólo cuando sirve para abrir una cerradura, cualquiera que sea su clase. Por eso que pueda estimarse que cuando abre el habitáculo donde se encuentra el cajero el hecho integra el robo, pero no cuando sirve únicamente para lograr la extracción del dinero. La solución todavía podría discutirse en los cajeros que tienen una tapa protectora que se abre al introducir la tarjeta, permitiendo la manipulación del mismo. En estos casos, sí podría entenderse que la tarjeta cumple la función de llave; pero no, desde luego, cuando su única utilidad es desencadenar

el proceso que termina en la entrega del dinero (125). En todo caso, cuando ello sea posible, la utilización de la misma con función de llave integrará la tentativa.

C. TRATAMIENTO PENAL DE LA MANIPULACIÓN DE LAS TARJETAS

La realización de algunos de los fraudes analizados presupone, aparte el conocimiento del número personal del titular, la manipulación de la banda magnética de la tarjeta, en donde se recogen datos que, de no ser alterados, impedirían la utilización de la misma (126). El problema que ello plantea es si puede considerarse que con la manipulación se produce, además del delito patrimonial que, en su caso, corresponda, una falsedad documental.

La jurisprudencia ha venido tratando a las tarjetas de crédito como documento mercantil (127), sin que la falsificación de las mismas encontrara, por tanto, inconveniente alguno para ser castigada. La duda surge porque aquí lo que se manipula no es el soporte material en sí, que permanece inalterable, ni siquiera la banda magnética en su realidad física, sino los datos que aparecen grabados en la misma, lo que plantea el problema de si cabe hablar de falsedad cuando se alteran sólo los impulsos electromagnéticos que se contienen en ficheros o documentos electrónicos.

Tradicionalmente, el concepto de documento se ha reservado para los elementos escritos en los que se recoge una declaración de voluntad atribuible a una persona o un hecho con trascendencia jurídica y destinado a entrar en el tráfico jurídico (128). La última jurisprudencia, sin embargo, evolucionó a un concepto material de documento en el que tenían cabida también otros objetos como grabaciones de vídeo, discos, cintas de audio o discos informáticos (129). Noción que constituye el antecedente del concepto que proporciona el art. 26 del Código penal, en el que, por encima de la forma, predomina la capacidad del objeto para probar algo o acreditar algún hecho con relevancia jurídica (130).

A los efectos que ahora interesan, lo más significativo es que el art. 26 declara que sólo puede ser documento lo que se halle recogido en un soporte material («se considera documento todo soporte material»), lo que supone excluir del concepto a los datos informáticos en cuanto tales (131). La razón es que al no ser directamente comprensible por el hombre la información que contienen, resultando precisa para ello la intermediación de la máquina, su validez queda subordinada a la posibilidad de ser reproducidos automáticamente sobre soportes que lo hagan entendible de manera inmediata (132).

En lo que se refiere a la manipulación de las tarjetas, el problema se plantea porque aquí lo único que se modifican son los datos de la banda magnética. Datos, que aunque tienen capacidad para probar hechos con trascendencia jurídica no son legibles directamente, razón por la que se ha considerado que la manipulación resultaría atípica (133). Frente a este criterio (134), creo que la nueva definición del concepto de documento que proporciona el art. 26 y, sobre todo, una visión funcional de las tarjetas de crédito permiten mantener que la alteración de los datos de la banda magnética puede dar lugar al delito de falsedad en documento mercantil. De una parte, porque la tarjeta es un todo y su valor documental proviene tanto del soporte plástico y de los datos que figuran impresos en el mismo como de los que están grabados en su banda magnética; y ambos resultan inseparables, sin que ninguno de ellos tenga valor autónomo por sí. De otra, y como consecuencia, porque se altera el soporte y los hechos con relevancia jurídica que expresa o incorpora (art. 26), o lo que es lo mismo, el documento, tanto si se cambian unos como otros. En ambos casos, por utilizar la útil y afortunada referencia del § 269 StGB (135), se produce una alteración de datos probatorios que, de ser directamente perceptibles, darían lugar a un documento falso.

NOTAS:

1 Sobre la situación en el Código penal anterior, vid. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en RFDUCM, Monográfico n.º 12, 1982, pp.107 y ss. y «Tratamiento penal de los ilícitos patrimoniales relacionados con medios informáticos», en PJ, Nuevas formas de delincuencia, n.º especial IX, pp. 86 y ss. La falta de respuesta legal adecuada no era, sin embargo, exclusiva del caso español, sino que constituía una realidad común a prácticamente todos los ordenamientos, que se vieron sorprendidos por el desarrollo de un fenómeno cuya extraordinaria progresión no habían previsto. Sobre la situación en los países más próximos y sobre las iniciativas legales que ello provocó, vid. BORRUSO, en AAVV, Profili penali dell´informatica, Milano, 1994, pp. 5 y ss; DEVÈZE, «Les qualifications pénales applicables aux fraudes informatiques», en Le droit criminel face aux technologies nouvelles de la comunication. Actes du VIIIº Congrès de l´Association Francaise de Droit Pénal organizé du 28 au 30 november 1985 à l´Université de Grenoble, París, 1986, pp. 185 y ss; BRIAT, «La delinquiance informatique: aspects de droit comparé», en Le droit criminel face aux technologies nouvelles de la comunication, cit., pp. 263 y ss.; MÖHRENSCHLAGER, «Tendencias de política jurídica en la lucha contra la

delincuencia informática», en MIR (Ed.), Delincuencia informática, Barcelona, 1992, pp. 47 y ss; ROMEO CASABONA, Poder informático y seguridad jurídica, Madrid, 1988, pp. 90 y ss.; CORCOY, «Legislación penal sobre protección de la criminalidad en distintos países europeos», en Delincuencia informática, cit., pp. 177 y ss.

2 Técnica legal, a mi juicio, preferible a la de creación de figuras delictivas orientadas directamente a la protección de sistemas informáticos, como ha hecho, por ejemplo, con gran minuciosidad, el Código penal italiano. Sobre las ventajas e inconvenientes de uno y otro procedimiento, vid., ROMEO CASABONA, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», en PJ, nº 31, 1993, pp. 180-181.

3 A pesar de que no hay estudios criminológicos suficientes para precisar el alcance de este tipo de delincuencia ni para realizar un cálculo relativamente preciso de la cifra negra propia de estas modalidades de delincuencia, si puede afirmarse que la criminalidad relacionada con sistemas o procedimientos informáticos ha alcanzado gran difusión en los últimos años (Vid. SARZANA,«Criminalitá e tecnologia: Il caso dei computer-crimes», en Rassegna Penitenciaria e Criminologica, 1979, p. 57; SNEYERS, El fraude y otros delitos informáticos, Madrid, 1990, pp.3 y ss., SICHER, pp.18 y ss.; en relación con España, la carencia de datos es prácticamente total, vid., por todos, CAMACHO LOSA, El delito informático, cit., pp. 69-82). Tampoco hay datos sobre la entidad de los perjuicios causados, aunque la coincidencia es unánime en que son muy altos y desde luego bastante superiores a los que provoca la delincuencia "tradicional" (vid., GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., p. 109). Lo que se ve agravado por el hecho de que el éxito de la primera manipulación, invita a que ésta se repita sucesivamente, lo que otorga a estos fraudes un efecto continuado que hace que los perjuicios lleguen a ser espectaculares (TIEDEMANN, Poder económico y delito, Barcelona, 1985, p.126). A la ignorancia de los efectos reales contribuye, sin duda, la gran dificultad que a menudo encuentra el descubrimiento de la dinámica del fraude y de su autor (vid., CAMACHO LOSA, El delito informático, cit., pp. 106-124) y el poco interés que los afectados tienen en ocasiones en su persecución, lo que haría pública la vulnerabilidad de sistemas que tienen gran interés en presentar como inexpugnables y en los que, sin embargo, no se han adoptado las debidas medidas de seguridad, tanto informáticas como de gestión y organización (vid., CAMACHO LOSA, El delito informático, Madrid, 1987, pp. 142 y ss.; SIEBER, «Documentación para una aproximación al delito informático», en Delincuencia informática, cit., pp. 83-89, por todos). Contra lo que a veces suele afirmarse, ni es precisa una inteligencia superior en el autor, ni se requieren elevados conocimientos técnicos, sino que se trata de comportamientos capaces de ser desarrollados por cualquiera mínimamente introducido en el manejo de ordenadores, incluso domésticos. Los conocidos casos de jóvenes que, casi a modo de juego, se introducen en sofisticados sistemas informáticos es prueba más que significativa de ello. Según estudios desarrollados en relación con los casos conocidos en Estados Unidos y Alemania Federal, los autores suelen ser personas jóvenes (entre 24 y 35 años), instruidos, casi siempre varones, sin antecedentes penales, despiertos, muy activos, impacientes y muy motivados, que actúan por muy diversos motivos (venganza, ánimo de lucro, afán de notoriedad o simplemente respuesta al "reto" permanente a la inteligencia que significa el ordenador y que tan frecuente resulta entre quienes trabajan habitualmente con ellos) y a menudo en grupo (aunque difícilmente integrado por programadores y operadores, dada la característica rivalidad entre ambos) (cfr. SARZANA, «Criminalitá e tecnologia: ...», cit., pp. 76-77). No es raro que resulten sugestionados por el síndrome de "Robin Hood", considerando inmoral el daño hecho a personas concretas, pero no el causado a organizaciones o empresas (Vid. SARZANA, op. cit., p. 74). Muy frecuentemente los medios que utilizan no son considerados ilegales en el ambiente informático (copias ilegales de programas, intercambios no autorizados de programas, introducirse en sistemas informáticos por diversión, utilizar el sistema para fines propios, etc.), considerando que a lo sumo tales comportamientos pueden resultar "irregulares", tal vez un simple "juego", pero en ningún caso ilícitos (vid. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., pp. 110-111; CAMACHO LOSA, El delito informático, cit., pp. 74 y ss.; GUTIÉRREZ FRANCÉS, Fraude informático y estafa, Madrid, 1991, pp. 74 y ss.). Característica, por lo demás, propia de la delincuencia de cuello blanco y de gran interés a efectos de los mecanismos de asociación diferencial (SARZANA, «Criminalitá e tecnologia: ...», cit., pp. 75 y ss.).

4 Ni otras implicaciones de gran interés, como las consecuencias en la criminalidad organizada (vid., AAVV, Informatica e criminalitá organizzata. Atti della Tavola Rotonda organizzata a Palermo il 4-2-1984, Milano, 1988, passim), o en la aplicación de la ley penal en el espacio (vid. MASSE, en AAVV, Profili dell´informatica, Milano, 1994, pp. 282 y ss.).

5 Apelando a la gesta mítica de Ulises, el caballo de Troya supone introducir dentro de un programa de uso habitual una rutina no autorizada que provoca que el programa actúe en las ocasiones que define el manipulador de forma distinta a como debía, realizando operaciones no previstas (borrar ficheros, alterar datos, ordenar pagos, bloquear el sistema, etc.). Su realización requiere conocimientos informáticos y la posibilidad de acceder a los programas de uso común, siendo un comportamiento frecuente en empleados descontentos. Aunque es fácil de prevenir, su descubrimiento es difícil, porque el intruso puede prever incluso la autodestrucción de la rutina, una vez que cumplió su función (vid., SNEYERS, El fraude y otros delitos informáticos, cit., p. 115).

6 Con esta referencia genérica se conocen los accesos a sistemas privados a través de las redes públicas de transmisión de datos, burlando las medidas de seguridad dispuestas en el sistema que se vulnera (vid. un muy ameno y documentado análisis del fenómeno en CLOUGH-MUNGO, Los piratas del chip, Barcelona, 1992, passim, y en particular, pp. 61 y ss. y 195 y ss.).

7 Se denomina así al uso no autorizado de utilidades que permiten acceder a cualquier lugar del sistema informático, por protegido que esté, lo que faculta al sujeto para borrar, copiar, insertar o utilizar datos almacenados en el mismo. Su realización sólo está al alcance de programadores o de analistas de sistemas, que han de conocer bien su funcionamiento. El descubrimiento de su utilización es muy difícil porque no dejan constancia del acceso en los ficheros de control que recogen las operaciones diarias realizadas con el ordenador (logging, journal y archivos semejantes), por lo que no dejan rastro de quién lo realiza, pudiéndose hacer aparecer las consecuencias producidas como errores del programa (vid., CAMACHO LOSA, El delito informático, cit., pp. 42-44).

8 Consiste en la recogida de información residual, física (manuales, diagramas, notas de programación, etc.) o lógica (ficheros residuales, temporales, etc.) para conocer las formas de acceder al sistema (vid. SNEYERS, El fraude y otros delitos informáticos, cit., pp. 110-113).

9 Las puertas falsas son vías de acceso a programas que se dejan intencionadamente abiertas por los creadores o encargados del mantenimiento del mismo con el fin de poder probarlos y verificar su funcionamiento antes de su instalación definitiva y de las que generalmente no queda constancia en la documentación del mismo. En teoría, deberían suprimirse, pero unas veces con vistas a su eventual utilización futura y las más por olvido o desidia, se dejan abiertas (vid., CAMACHO LOSA, El delito informático, cit., pp. 44-46; SNEYERS, El fraude y otros delitos informáticos, cit., p. 116).

10 El procedimiento consiste en entrar en el sistema a través de personas autorizadas, ya haciéndose pasar por ellos (porque se han descubierto sus claves de acceso -password), ya aprovechando los momentos en los que los mismos acceden al sistema, abren líneas de comunicación, etc. (cfr. SNEYERS, El fraude y otros delitos informáticos, cit., p. 116).

11 Además de los procedimientos específicos de comisión de otros delitos como los daños (mediante virus, bombas lógicas o ataques asíncronos) o fraudes patrimoniales o transferencias electrónicas de fondos (técnica del salami) que serán comentadas al tratar de los mismos.

12 Sobre las distintas clasificaciones, vid. ROMEO CASABONA, Poder informático y seguridad jurídica, cit., pp. 43-46; GUTIÉRREZ FRANCÉS, Fraude informático y estafa, cit., pp. 58 y ss.; RUIZ VADILLO, «Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica», en Nuevas formas de delincuencia, PJ, nº especial IX, pp. 64 y ss.

13 Vid. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., pp. 116-117.

14 La parte física (hardware) del sistema informático se conforma con los elementos mecánicos o electrónicos necesarios para su funcionamiento (unidades de proceso, teclados, monitores, unidades de lectura-escritura para almacenamiento de información, transmisión de datos, impresoras, etc.). La parte lógica la integran tanto los programas (software: sistema operativo -que controla los elementos del sistema y permite realizar las operaciones elementales- y aplicaciones -que llevan a cabo tareas específicas de tratamiento de la información: nóminas, contabilidades, proceso de textos, etc.), como los ficheros y archivos en los que se almacena la información que se suministra al ordenador o los datos obtenidos con las aplicaciones específicas. También aparecen referidos a los elementos lógicos los Manuales o Libros de Usuario en los que se explican los programas y aplicaciones. Su naturaleza corporal, sin embargo, determina que a efectos penales deban ser considerados como elementos físicos y no lógicos (vid. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., pp. 113 y ss).

15 En lo que se refiere a las modalidades de apoderamiento, tales objetos, en cuanto corporales, económicamente valorables y susceptibles de desplazamiento y apropiación, son «cosas muebles» cuya separación fáctica del patrimonio de una persona para incorporarlas al del agente puede integrar los delitos de hurto o robo (para mayor detalle, vid. GONZÁLEZ RUS, en CARMONA SALGADO, GONZÁLEZ RUS, MORILLAS CUEVA, POLAINO NAVARRETE, PORTILLA CONTRERAS, Curso de Derecho penal español, Parte Especial, I, dirigido por COBO DEL ROSAL, Madrid, 1996, pp. 559 y ss. y 594 y ss.). Respecto de las circunstancias de agravación aplicables al hurto y al robo con fuerza en las cosas (arts. 235 y 241.1), las que en principio aparecen más relacionadas con estos supuestos son la segunda (art. 235.2), relativa al apoderamiento de cosas destinadas a un servicio público, si se produjera un grave quebranto al mismo, y la tercera (art. 235.3), cuando el hurto o el robo con fuerza revista especial gravedad, atendido el valor de los efectos sustraídos o se produzcan perjuicios de especial consideración, lo que dependerá de las particularidades de cada caso. Únicamente debe insistirse en la necesidad de que se produzca efectivamente la «grave perturbación» del servicio -lo que en estos casos no tendrá nada de extraordinario- y que la importancia económica de los perjuicios que pueden derivarse para el sujeto pasivo de la sustracción puede llegar en ocasiones a cantidades superiores al propio precio del sistema (para un estudio más detenido de ambas circunstancias, vid., GONZÁLEZ RUS, Curso, I, cit., pp. 586-587). Tampoco ofrece particularidades dignas de mención la aplicación de la estafa: mediando engaño bastante y perjuicio, el delito se producirá, teniendo presente que objeto material puede ser cualquiera de los elementos integrantes del patrimonio, ya se trate de una cosa corporal, mueble o inmueble, o de un derecho (vid. GONZÁLEZ RUS, Curso, I, cit., pp. 652 y ss.). Y lo mismo sucede con la apropiación indebida, que será apreciable cuando quien ha recibido uno de los elementos físicos del sistema con obligación de devolverlos se apropia de ellos (pp. 695 y ss.). Debe recordarse, sin embargo, que para su integración no basta con un simple mal uso de la cosa poseída, sino que son precisos verdaderos actos de apropiación. La que podría llamarse "apropiación indebida de uso" sólo resulta punible en la medida en que resulte incluible en el art. 256, que estudiamos a continuación. Igualmente, debe advertirse que por la estructura de los centros de proceso de datos, que suelen gozar de una notable autonomía funcional y quienes trabajan en ellos de una gran independencia y capacidad de disposición sobre el sistema y sus elementos, cuando la apropiación del elemento físico se produzca por estas personas (analistas, programadores, operadores) pueden plantearse interesantes problemas de calificación, que ofrecen todas las dificultades tradicionales que presenta la distinción entre el hurto y la apropiación indebida en los casos de los llamados "servidores de la posesión" (criada, cajero, etc.; vid. GONZÁLEZ RUS, op. cit., pp. 693-696 y 703-706). En cuanto a las agravaciones del art. 250, aplicables tanto a la estafa como a la apropiación indebida de cuantía superior a cincuenta mil pesetas, la única que puede suscitar alguna duda específica en relación con los sistemas o elementos informáticos es la del supuesto 1.º, en particular si pueden calificarse o no de cosas de primera necesidad o bienes de reconocida utilidad social, lo que no parece que sea aplicable a los elementos informáticos. Las demás no ofrecen particularidad alguna (cfr., GONZÁLEZ RUS, Curso, I, cit., pp. 676-678). Respecto de los daños, me remito a lo que se diga más adelante.

16 GONZÁLEZ RUS, Curso, I, cit., pp. 784 y ss.
17 Su trascendencia es tal que han sido utilizados incluso con finalidades políticas y terroristas, vid., CAMACHO LOSA, El delito informático, cit., pp. 97-105.
18 Vid. GONZÁLEZ RUS, Curso, I, cit., pp. 751 y ss. La importancia económica de los equipos informáticos y, sobre todo, el papel de extraordinaria importancia que actualmente tienen en la gestión, hacen posible que la destrucción del sistema o de elementos fundamentales del mismo alcance cantidades superiores a los diez millones de pesetas, lo que permitirá la aplicación de los daños imprudentes (art. 267). Igualmente, tampoco debe descartarse la aplicación del supuesto 5.º del art. 264 (que se arruine al perjudicado o se le coloque en grave situación económica).
19 La distinción entre los daños a los sistemas en sí y a los datos es el que sigue el Código austríaco, cuyo § 126 a.1 castiga con la pena de privación de libertad de hasta seis meses o con pena de multa de hasta 360-días a «Quien perjudicare a otro a través de la alteración, cancelación, inutilización u ocultación de datos protegidos automáticamente, confiados o transmitidos, sobre los que carezca, en todo o en parte, de disponibilidad». El StGB alemán, aunque distingue entre el § 303 a. (alteración de datos) que castiga a «Quien ilícitamente cancelare, ocultare, inutilizare o alterare datos» (privación de libertad de hasta dos años o multa), y el § 303 b. (sabotaje informático) que castiga con pena de privación de libertad de hasta cinco años o con multa a «Quien destruya una elaboración de datos de especial significado para una fábrica ajena, una empresa o una administración pública, a través de ... la destrucción, deterioro, inutilización, eliminación o alteración de un sistema de elaboración de datos o de los portadores de los datos», en éste se comprende tanto la destrucción de equipos como la de soportes de datos y simples elementos lógicos (vid., MÖHRENSCHLAGER, «Tendencias de política jurídica ...», cit., pp. 63 y ss.). En una línea semejante, el Código italiano castiga conjuntamente los daños que se produzcan en los elementos físicos y lógicos. En este sentido, el art. 420 en donde se recoge el Atentado a instalaciones de utilidad pública: «El que realice un hecho dirigido a dañar o destruir instalaciones de utilidad pública, será castigado, salvo que el hecho constituya un delito más grave, con la reclusión de uno a cuatro años. La misma pena se aplicará a quien realice un hecho dirigido a dañar o destruir sistemas informáticos o telemáticos de utilidad pública, o los datos, informaciones o programas contenidos o pertenecientes a ellos. Si del hecho se deriva la destrucción o el daño de la instalación o del sistema, de los datos, de las informaciones o de los programas o la interrupción, incluso parcial, del funcionamiento de la instalación o del sistema, la pena será de reclusión de tres a ocho años.» (vid., AAVV, Profili penali dell´informatica, cit., pp.83 y ss.).
20 La aproximación de un simple imán a un disco magnético, golpear o mover el ordenador cuando se están grabando los datos, un corte en el suministro de energía eléctrica o alteraciones intermitentes de tensión, aumento o descenso de la temperatura o la humedad más allá de los límites de funcionamiento óptimo del sistema, pueden suponer pérdidas y perturbaciones importantes en el almacenamiento de los datos capaces de dañarlos.
21 Los virus son programas informáticos diseñados específicamente para realizar dos funciones: replicarse de un sistema informático a otro y situarse en los ordenadores de forma que pueda destruir o modificar programas y ficheros de datos, interfiriendo los procesos normales del sistema operativo (vid. SNEYERS, El fraude y otros delitos informáticos, cit., pp. 101-105). El alto número y variedad de los mismos, su extraordinaria capacidad de contagio y los grandes daños que pueden producir explica la atención y preocupación que han provocado. Sobre casos reales y su diferencia con las bombas lógicas, los gusanos, y la técnica del caballo de Troya, vid., CLOUGH-MUNGO, Los piratas del chip, cit., pp. 127 y ss. con una detallada exposición del nacimiento y desarrollo del fenómeno; datos criminológicos y casos reales pueden verse también en SIEBER, «Criminalidad informática: Peligro y prevención», cit., pp. 25-27 y «Documentación para una aproximación al delito informático», cit., pp. 74-77; CORCOY, «Protección penal del sabotaje informático. Especial consideración de los delitos de daños», en MIR (ed.) Delincuencia informática, cit., pp. 148 y ss.
22 Se conocen como tales ciertas rutinas o modificaciones de programas que producen las modificaciones, borrados de ficheros o alteraciones del sistema en un momento posterior a aquél en el que se introducen, cuando se llega a una determinada fecha o se realiza una cierta operación. Son parecidos al caballo de Troya, aunque la finalidad que se persigue con las bombas lógicas es primordialmente la de dañar el sistema o los datos; aunque pueden utilizarse también para ordenar pagos, realizar transferencias de fondos, etc. La experiencia muestra que son el procedimiento preferido por empleados descontentos que programan su explosión para un momento en el que ellos ya no se encuentran en la empresa (vid., CAMACHO LOSA, El delito informático, cit., pp. 47-48; SNEYERS, El fraude y otros delitos informáticos, cit., pp. 113-114, por todos).
23 Como el de los denominados ataques asíncronos, que suponen modificaciones del sistema operativo y sus relaciones con las aplicaciones con el fin de impedir la recuperación de datos cuando se interrumpe la ejecución de un programa (CAMACHO LOSA, El delito informático, cit., pp. 48-51). O la simple eliminación de comentarios en los programas, lo que hace prácticamente imposible su revisión por quien no lo haya confeccionado. Para que se produzcan los daños ni siquiera es preciso destruir o borrar toda la información almacenada, bastando en ocasiones con eliminar o alterar determinados ficheros, cambiar códigos de acceso y contraseñas (password), introducir datos falsos en directorios y ficheros maestros, que resultan necesarios para el acceso a la información, borrar ciertas rutinas de los programas, introducir sentencias equivocadas, etc.
24 Así el art. 615.5 del Código penal italiano, en el que se castiga con la pena de reclusión de hasta dos años y multa de hasta veinte millones de liras la difusión de programas que tengan por objeto o produzcan el efecto de dañar un sistema informático o telemático, los datos o los programas contenidos en él o pertenecientes al mismo o la interrupción, total o parcial, o la alteración de su funcionamiento (vid. BUONOMO, en AAVV, Profili penali dell´informnatica, cit., pp. 82 y ss.).
25 El rechazo se basaba en una mala comprensión del requisito de la "corporalidad" o "materialidad" que se exigía al objeto material del delito de daños (para mayor detalle, vid., GONZÁLEZ RUS, «Aproximación al tratamiento penal de

los ilícitos patrimoniales ...», cit., pp. 138-142).
26 Precisamente el no ser directamente perceptibles es la característica más peculiar de los mismos. Expresamente así los define el § 202 a.2 StGB: «Se consideran datos ... sólo aquéllos electrónicos, magnéticos o que están almacenados de forma no inmediatamente perceptible o que son transmitidos.»
27 Únicamente quedan excluidas las cosas carentes de valor económico, porque sólo en atención a éste puede determinarse la «cuantía del daño», que delimita el delito de la falta y la gravedad de la pena, y puede considerarse a los daños un delito contra el patrimonio (cfr., por todos, JORGE BARREIRO, «El delito de daños en el Código penal», en ADPCP, 1983, p. 513 y GONZÁLEZ RUS, Curso, I, cit., p. 755).
28 El apartado no resuelve, sin embargo, el problema de los daños causados en otros elementos inmateriales, como grabaciones sonoras o audiovisuales, que también son impulsos electromagnéticos y, por tanto, inmateriales. Personalmente, creo que, aún sin mención expresa, ni hubo antes ni hay ahora inconveniente alguno en aplicar el delito en estos casos, en términos semejantes a los dispuestos para los elementos informáticos. Y es que la dinámica del delito de daños se construye en torno a la posibilidad de destrucción o deterioro de la cosa, por lo que -como ya se ha dicho- puede ser eventual objeto del delito todo aquello que, corporal o incorporal, tenga valor económico, sea capaz de fundamentar un derecho de propiedad y pueda ser dañado. Entre otras cosas, porque sería absurdo que pudiera integrar el delito la destrucción de un fichero informático en el que se recoge una aplicación multimedia, con vídeos y sonido, y que ello no fuera posible cuando lo que se hace es borrar directamente una grabación fijada en cualquier soporte audiovisual.
29 GIANNANTONIO, Manuale di diritto dell´informatica, 1994, p. 339.
30 Vid. BORRUSO, Profili penali dell´informatica, cit., p. 27 y SNEYERS, El fraude y otros delitos informáticos, cit., p. 111.
31 En sentido estricto, sistema informático es un conjunto de elementos dotados de un grado de estructuración y complejidad superior al de un ordenador personal (BUONOMO, en Profili penali dell´informatica, cit., pp. 69 y 149). Sin embargo, esa acepción no puede ser la acogida aquí, pues ello supondría restringir demasiado el ámbito del delito.
32 De hecho, en la doctrina alemana se considera que el borrado de datos propios es punible cuando el procesamiento de los mismos ha sido realizado por terceros, así como la destrucción de equipos por el propietario, cuando en ellos tenga un tercero interés legítimo; vid., MÖHRENSCHLAGER, «Tendencias de política jurídica ...», cit., p. 63.
33 Como consecuencia, no habría delito de daños cuando se libera a un animal del lugar en donde lo tiene encerrado el propietario, cuando se deja abierto el grifo de un tonel de vino, cuando se desinflan las ruedas de un coche, se arroja una joya al mar, etc., puesto que con ello no se altera la esencia de la cosa (así, por todos, MUÑOZ CONDE, Derecho Penal, PE, Valencia, 1996, p. 415).
34 Cfr. JORGE BARREIRO, «El delito de daños en el Código penal», cit., p. 513, por todos.
35 Así, mientras que habría que apreciar un delito daños cuando se sueltan animales, o se arroja una joya al mar, puesto que la cosa se pierde o desaparece, lo que hace los supuestos equivalentes a los de destrucción, no habría tal cuando simplemente se pone un cepo al coche, se desinfla una rueda o un balón, porque el comportamiento, aún afectando al valor de uso, no determina una afectación de la sustancia que suponga una pérdida de valor real de la cosa, lo que -como ya se ha dicho- resulta imprescindible para determinar la cuantía conforme a la que tipificar el hecho (vid. GONZÁLEZ RUS, Curso, I, cit., pp. 752-753).
36 Se citan como ejemplo los casos de la destrucción de un mueble inservible cuya transformación en madera hace aumentar su valor como combustible (y, por tanto, globalmente considerado, un enriquecimiento del patrimonio del dueño), la eliminación del viejo caballo cuyo mantenimiento resultaba costoso al propietario y cuya muerte le libera de gastos, etc.; casos que, a pesar de no comportar un perjuicio patrimonial efectivo, se califican como daños. Así, la posición dominante; vid. por todos, JORGE BARREIRO, «El delito de daños en el Código penal», cit., p. 515, MUÑOZ CONDE, Derecho Penal, PE, cit., p. 414, GONZÁLEZ RUS, Curso, I, cit., pp. 751-752. Que el art. 264.5º agrave la pena cuando los daños «arruinen al perjudicado o se le coloque en grave situación económica», contemplando, por tanto, el empobrecimiento del patrimonio ajeno como causa del delito, y que el art. 263 se refiera indistintamente a la hora de fijar la pena a «la condición económica de la víctima y la cuantía del daño», no contradice la conclusión expuesta. En el primer caso, porque tal previsión es perfectamente coherente con los principios político-criminales en los que se inspira en general el Código para la punición de los delitos contra la propiedad. Baste recordar que también la causación de perjuicios de especial consideración o la grave situación económica de la víctima se utilizan como agravantes en el hurto, en el robo con fuerza, en la estafa y en la apropiación indebida, sin que ello prejuzgue la cuestión de si es necesario o no el perjuicio efectivo para su consumación, que se decide en atención a otros aspectos. En el caso del art. 263, porque a pesar de la mención dual, lo relevante sigue siendo la cuantía del daño, que es lo que se toma en cuenta para la diferenciación entre el delito y la falta.
37 Visto desde la perspectiva exclusiva de los elementos físicos del sistema, la destrucción de datos no supone alteración alguna en la sustancia, pues un disco o una cinta magnética con un fichero grabado no son distintos de un disco o de una cinta virgen. De hecho, al borrar el fichero lo que se hace es sustituir los impulsos magnéticos originales por otros, sin alterar la composición físico-química de la materia. Del mismo modo, la memoria del ordenador tampoco se ve alterada en su sustancia al eliminar la información que contiene, pues lo único que se hace es modificar el estado de activación de los circuitos que la integran. Por ello, que el ordenador pueda continuar funcionando perfectamente o que el soporte físico en que se almacenan los datos siga sirviendo para el objeto al que aparece destinado (un disco del que se borra un fichero puede seguir almacenando otros) resulta indiferente en orden a la apreciación de esta modalidad de daños. Como ya se ha dicho, cuando se borra un fichero de datos o un programa no puede decirse que no hay alteración en la sustancia, en cuanto que la información que resulta destruida es la sustancia misma del objeto dañado. Que los elementos lógicos en sí mismos no puedan ser operativos sin un ordenador, no dice nada en contra de su autonomía a efectos de tutela. Entenderlo

de otra manera, considerando que los elementos lógicos no tienen sentido sino dentro de los elementos físicos, y que el daño a los mismos sólo es relevante en la medida en que incide en el funcionamiento o sustancia del conjunto, desconoce la realidad de las cosas y de las propias valoraciones legales.

38 Salvo las rutinas y programas que integran el "sistema operativo" del ordenador, la destrucción o inutilización de los elementos lógicos no afecta a la integridad del sistema informático, que sigue conservando su plena capacidad de funcionamiento. El daño, por consiguiente, no puede verse sólo desde la perspectiva global del funcionamiento del sistema o de sus elementos físicos, sino también, según los casos, desde la propia de los elementos físicos y lógicos que lo integran y que pueden resultar recíprocamente autónomos a efectos de valoración y protección.

39 La posibilidad de apreciar un concurso de delitos entre los daños a los elementos físicos (art. 263) y los que afecten a lógicos (art. 264.2) queda descartada de antemano, al referirse éste a daños que van recogidos en soportes, comprendiendo, pues, los que suponen la destrucción de unos y otros.

40 Así, MÖHRENSCHLAGER, «Tendencias de política jurídica ...», cit., pp. 140-141.

41 La posibilidad de recuperar los datos debe apreciarse desde la perspectiva del usuario medio, con los recursos ordinarios a disposición del mismo. En todo caso, si la restauración de los elementos afectados fuera posible por personal experto, recurriendo a más o menos sofisticados medios o procesos técnicos, podría apreciarse la tentativa.

42 Así también CORCOY, «Protección penal del sabotaje informático...», cit., p. 174.

43 De la misma opinión ROMEO CASABONA, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», cit., p. 203, que añade los casos en los que hubiera copias impresas.

44 Vid., CLOUGH-MUNGO, Los piratas del chip, cit., pp.61 y ss. y 195 y ss.; CAMACHO LOSA, El delito informático, cit., pp. 61-67; SNEYERS, El fraude y otros delitos informáticos, cit., pp. 66-94; SIEBER, «Documentación para una aproximación al delito informático», cit., pp. 72-74 y 77-78, por todos.

45 Así, el § 202 a StGB (Espionaje de datos): «Quien sin autorización se procure a sí mismo o a otro datos especialmente asegurados contra ilícitas intromisiones» (pena privativa de libertad de hasta tres años o pena de multa). A estos efectos, se consideran datos «sólo aquéllos electrónicos, magnéticos o que están almacenados de forma no inmediatamente perceptible o que son transmitidos» (vid., MÖHRENSCHLAGER, «Tendencias de política jurídica ...», cit., pp. 60-61 y «El nuevo Derecho penal informático en Alemania», en MIR (ed.), Delincuencia informática, cit., pp. 135-138). Igualmente, el art. 615-ter del Código penal italiano: «Acceso abusivo a un sistema informático o telemático): El que abusivamente se introduce en un sistema informático o telemático protegido por medidas de seguridad o se mantiene en él contra la voluntad expresa o tácita de quien tiene el derecho de excluirlo, será castigado con la reclusión de hasta tres años.»; pena que se verá agravada, entre otras causas, si del acceso se deriva la destrucción o el deterioro del sistema o la interrupción total o parcial de su funcionamiento o el daño de los datos, las informaciones o los programas en el mismo contenido. Más allá de lo que es ordinario en la punición de comportamientos relacionados con la informática, el art. 615-quarter castiga a quien con la finalidad de procurarse para sí o para tercero un provecho o de causar un daño a otro, abusivamente se procura, reproduce, difunde o comunica códigos, palabras clave u otros medios idóneos para el acceso a un sistema informático o telemático protegido por medidas de seguridad, o proporciona indicaciones o instrucciones idóneas para ello (prisión hasta un año y multa hasta diez millones de liras (vid. BORRUSO, en Profili penali dell´informatica, cit., pp. 28 y ss.).

46 Si la información que contienen los archivos a los que se accede ilegítimamente hace referencia a datos reservados relacionados con la intimidad o la privacidad del titular, los preceptos eventualmente aplicables serán los relativos a los delitos contra la intimidad y el derecho a la propia imagen, que extienden la protección a las personas jurídicas (art. 200) y que no interesan a estos efectos. Si la conducta se realizara por funcionarios respecto de datos cuya custodia le está encomendada, los preceptos eventualmente invocables serían los arts. 413 y ss. Si los datos pueden ser calificados de secretos e informaciones relativas a la defensa nacional, las figuras que han de considerarse son las de los arts. 583, 584 y 598 y ss. Con esto no quiere decirse que estos delitos sean efectivamente aplicables; por el contrario, lo que indico es que las posibilidades de integrar un ilícito penal en estos casos depende de la interpretación de las figuras que se señalan, en la medida en que lo consientan.

47 Si además de descubrir el secreto, el sujeto lo difundiere, revelare o cediere a terceros, será de aplicación el art. 278.2. Cuando éstas últimas conductas se realicen por quien tiene legal o contractualmente obligación de guardar reserva, deberá tenerse en cuenta el art. 279. Y si los hechos se realizaren por quien no intervino en el descubrimiento, pero conoce el origen ilícito del secreto de empresa, el precepto invocable será el art. 280. Para un estudio más detenido de los mismos, vid. GONZÁLEZ RUS, Curso, I, cit., pp. 796 y ss.

48 Cuyo sentido ya conocemos, vid. infra II.1.

49 No se comprenden tampoco los casos en que se transcriben en papel, porque ya se trataría de «documentos escritos» o de «otros objetos que se refieran al mismo».

50 Dudando que estos comportamientos pudieran incluirse en el precepto semejante del Proyecto de 1992, GUTIÉRREZ FRANCÉS, «Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa», en ARROYO ZAPATERO-TIEDEMANN, Estudios de Derecho Penal económico, Universidad Castilla-La Mancha, 1994, pp. 196-197.

51 La copia ilícita de un programa de ordenador (software) ofrece particularidades propias, por lo que será tratado al ocuparnos de la protección penal de éstos.

52 Incluso desde el punto de vista del apoderamiento no habría problema alguno para incluir en el hurto estos supuestos, dado el sentido amplio en que se concibe el mismo, configurado no tanto como desplazamiento material, sino patrimonial. Si se admite como forma de apoderamiento la que se produce por medios mecánicos o químicos, no se ve porqué no

habría de comprender la realizada por medios informáticos (vid., GONZÁLEZ RUS, Curso, I, cit., pp. 563-566).
53 En términos naturalistas, «cosa» es cualquier objeto del mundo exterior, acogiendo a todo lo que tiene existencia corporal o espiritual, real, abstracta o imaginaria, resultando indiferente, en su caso, el estado de agregación de la materia (sólido, líquido o gaseoso). Así, en sentido genérico, cosas son, además de los objetos corpóreos, y por referir únicamente los ejemplos que resultan más discutidos, el agua, los gases, la electricidad y las energías en general (vid. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., p. 130). Desde esta perspectiva, por tanto, los ficheros informáticos son una cosa.
54 De hecho, en las defraudaciones no se requiere que el objeto material del delito sea una «cosa», o en los daños no es preciso que sea un objeto "corpóreo", en el sentido de "tangible", mientras que tales condiciones, y, más aún, la aprehensibilidad del objeto, constituye el elemento definidor de otras modalidades delictivas en las que se precisa su desplazamiento material, por lo que el concepto dependerá de las características típicas de cada delito.
55 Vid. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., pp. 130-133 y Curso, I, cit., pp. 566-567. Por esta razón no pueden ser objeto material del delito de hurto las energías y las fuerzas naturales (el calor, la luz, el viento, el fuego, las mareas), los derechos, las expresiones de ideas, las declaraciones de voluntad, los pensamientos y concepciones artísticas o la prestación de un aparato automático no consistente en un objeto. Sí lo es, en cambio, la escritura o cualquier representación gráfica que haga que la entidad inmaterial venga fijada permanentemente en una cosa aprehensible, que pierde entonces su valor en sí misma, para adquirir el que le comunica el contenido ideal en ella fijado, pudiendo ser objeto de apropiación en cuanto reúne todos los caracteres de cosa aprehensible y con un valor derivado del contenido inmaterial que encierra (títulos al portador, por ejemplo). Tampoco pueden ser objeto material de los delitos de apoderamiento aquéllas otras cosas que, siendo corporales (como los líquidos o los gases), no son en sí mismas susceptibles de desplazamiento patrimonial, resultando necesario que se encuentren en condiciones que permitan el apoderamiento o la apropiación (en bombonas, por ejemplo). En cuanto tales, sin embargo, y sin necesidad de que vayan en recipientes, podrán ser objeto material de las defraudaciones.
56 Muy simplemente expuesta, puede decirse que la "memoria" del ordenador se compone de miles o millones de circuitos eléctricos (según su capacidad), que reconocen si pasa (asignando el valor "1") o no pasa (asignándole el valor "0") la corriente por uno de ellos. Cada uno de esos circuitos elementales recibe el nombre de bit. La agrupación de 8 bits, resulta un byte, octeto o carácter, que permite ser asignado a una letra, número o cualquier signo y que admite hasta 256 combinaciones distintas. La distinta activación de cada uno de los bits (circuito activado o desactivado) que componen el byte, en un determinado orden, da lugar a un carácter diferente (por ejemplo: "0100 0001"= A; "0100 0010"= B, etc.), que aunque se representa en forma de números binarios, será interpretado y mostrado por el ordenador (en pantalla o impresora) por el carácter o símbolo correspondiente. Igualmente, los datos se almacenan en las memorias auxiliares (de muy diversa estructura: discos, cintas, cartuchos, "discos duros", CD-rom, etc.), que permiten grabar información en un soporte físico recubierto de material magnético, de forma semejante a como se hace en una cinta de audio ordinaria. Por eso que los elementos lógicos, los datos, la información, los programas, puedan ser concebidos como una especie de "flujo electromagnético".
57 La calificación de cosa mueble a la electricidad, ha sido, como es sabido, objeto de profunda polémica. Un sector doctrinal (fundamentalmente de la doctrina alemana), siguiendo a físicos y civilistas, vino considerándola como una "vibración", un "movimiento", una "fuerza de la materia" que no podía ser considerada "cosa" susceptible de integrar los delitos de hurto y robo. De la energía eléctrica, se decía, no nos podemos posesionar, tan sólo servirnos de ella para nuestros fines. Frente a este criterio, otro grupo de autores (fundamentalmente de la doctrina francesa), sobre la base de la inseparabilidad de energía y materia, mantenía la naturaleza de cosa de la energía eléctrica, porque también lo son los elementos incorporales y porque era susceptible de posesión (vid., por todos, FERRER SAMA, «Apropiación indebida», en NEJ, II, 1950, p. 765; MORILLAS CUEVA, «Defraudaciones de fluido eléctrico», en RGLJ, 1981, pp. 531 y ss.). En la doctrina española, las opiniones estuvieron igualmente divididas. QUINTANO RIPOLLÉS, Tratado de la Parte Especial del Derecho penal, II, Madrid, 1964, p. 1033), advertía que la incorporeidad de la energía eléctrica, con un valor económico concreto y perfectamente divisible, permitía considerarla como un bien o cosa, aunque fuera dudosa su inclusión dentro de las muebles o inmuebles, y aún su consideración como cosa corporal o incorporal; de una parte, porque al no poder ser materialmente aprehendida, la incorporeidad parece evidente, de otra, porque al ser susceptible del más cómodo de los manejos y fraccionamientos, nada impide afirmar su corporalidad. FERRER SAMA (op. cit., p. 765), en sentido parecido, estimaba que al admitirse en Derecho penal dentro del concepto de cosa tanto a las materiales como a las inmateriales, no existía dificultad alguna para considerar a la energía como "cosa", ya que tiene un valor, es de posible apropiación o utilización y las apropiaciones o defraudaciones ilícitas de la misma pueden causar un perjuicio. La jurisprudencia se pronunció a favor de esta tesis, optando por la naturaleza material y mueble de la electricidad, que si no es tangible, es al menos aprehensible, susceptible de trasladarse útilmente de un lugar a otro, por lo que los aprovechamientos subrepticios de gas y la electricidad podían ser incluidos en el hurto (vid., RODRÍGUEZ DEVESA, «Defraudaciones de fluido eléctrico y análogas», en NEJ, IV, 1954, p. 366). Otro sector doctrinal, en cambio, criticando la posición expuesta, consideró que, en cuanto energía, la electricidad no es una cosa corporal, por lo que no podía ser objeto del hurto o robo (RODRÍGUEZ DEVESA, op. cit., 365, y «Hurto», en NEJ, IX, 1962, p. 190, por todos).
58 Vid. infra II.1 y nota 25.
59 En el mismo sentido, ROMEO CASABONA, Poder informático y seguridad jurídica, cit., pp. 53-57 y «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», cit., p. 183; GUTIÉRREZ FRANCÉS, «Notas sobre la delincuencia informática ...», cit., pp. 187-188.
60 Para un análisis más detenido de los elementos del delito, con referencias a las posiciones doctrinales, vid., GONZÁLEZ RUS, Curso, I, cit., p.777 y QUINTERO OLIVARES, en QUINTERO OLIVARES (Dir.), VALLE MUÑIZ (Coord.), Comentarios a la Parte Especial del Derecho Penal, Pamplona, 1996, pp.570 y ss.

61 Vid. infra 3.A.a).
62 Para un estudio detenido me remito a GONZÁLEZ RUS, La protección penal de los programas de ordenador, libro inédito de próxima aparición.
63 En cuanto conjunto de datos o documento electrónico, los programas de ordenador pueden ser objeto material de los mismos comportamientos que quedan analizados en los apartados anteriores. Su destrucción podrá dar lugar a los daños. Si constituyera un «secreto de empresa» (antes de su comercialización, por ejemplo), a los delitos relativos al descubrimiento y revelación de los mismos. Igualmente, el "apoderamiento" tendrá el tratamiento que corresponde a cualquier otro fichero.
64 La posibilidad de proteger a los programas de ordenador a través de los delitos contra la propiedad industrial quedó expresamente descartada por la Ley de Patentes, que excluye su consideración como producto industrial y, de manera expresa, su patentabilidad (art. 4.2.c de la Ley 11/1986, de 20 de marzo, de Patentes). Sólo los programas que formen parte de una patente o de un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la LPI., de la protección que presta la propiedad industrial (art. 3.2 y 96.2 LPI.). Así lo reconoce expresamente el art. 96.3, párr. 2º LPI, al disponer que «Cuando los programas de ordenador formen parte de una patente o de un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial.». Lo que se reafirma en el art. 104 de la misma, al advertir que lo dispuesto en su Título VII respecto de los programas de ordenador «se entenderá sin perjuicio de cualesquiera otras disposiciones legales tales como las relativas a los derechos de patente, marcas, competencia desleal, secretos comerciales, protección de productos semiconductores o derecho de obligaciones.» Además, en la medida en que formen parte de una patente o de un modelo de utilidad podrán ser objeto material de falsificaciones, usurpaciones de patentes o, si están registrados con una marca, la usurpación de la misma o la utilización ilegítima de ella. Obsérvese que el programa en cuanto tal no es objeto de protección directa, sino que desde la perspectiva de la propiedad industrial lo que se tutelan son elementos conexos con el mismo (la marca; el dibujo, el modelo; la patente). Igualmente, el art. 3 LPI dispone que «los derechos de autor son independientes, compatibles y acumulables con: 1º. La propiedad y otros derechos que tengan por objeto la cosa material a la que está incorporada la creación intelectual. 2ª Los derechos de propiedad industrial que puedan existir sobre la obra. 3º Los otros derechos de propiedad intelectual reconocidos en el libro II de la presente Ley».
65 El Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes en la materia (B.O.E. n.º 97, de 22 de abril de 1996), da nueva redacción a los artículos 95 a 104, conforme a las previsiones de la Ley 16/1993, de 23 de diciembre, de incorporación al Derecho español de la Directiva 91/250/CEE, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador, que queda derogada. Igualmente, se incorpora a su articulado, y se deroga, la Ley 27/1995, de 11 de octubre, de incorporación al derecho español de la Directiva 98 de la CEE, de 29 de octubre de 1993, sobre armonización del plazo de protección del derecho de autor y determinados derechos afines. Sobre la situación antes de la Ley 16/1993, vid. ROMEO CASABONA, «La protección penal del software en el derecho español», en CPC, 1988, nº 35, pp. 317 y ss. y «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», cit., pp. 191 y ss.
66 De manera puramente ejemplificativa, se mencionan los libros, folletos, escritos y demás creaciones impresas, las composiciones musicales, obras teatrales de todo género, cinematográficas, esculturas, pinturas, dibujos, grabados y demás creaciones plásticas, diseños arquitectónicos y de ingeniería y científicos, fotografías, programas de ordenador y el título de la obra, cuando sea original (art. 10).
67 Sin embargo, la LPI. no les atribuye ninguna calificación específica, a diferencia de lo que establecía el art. 1 de la Ley 16/1993, que los consideraba como «obras literarias tal como se definen en el Convenio de Berna para la protección de obras literarias y artísticas».
68 Este último precepto advierte que «El autor, salvo pacto en contrario, no podrá oponerse a que el cesionario titular de los derecho de explotación realice o autorice la realización de versiones sucesivas de su programa ni de programas derivados del mismo.»
69 El mismo régimen sigue la reproducción de los resultados de tales actos [art. 99, párr. 1º, b) LPI.].
70 Del mismo modo, la traducción y la reproducción del código (descompilación) no necesitará de autorización del titular del derecho cuando la misma «sea indispensable para obtener la información necesaria para la interoperabilidad de un programa creado de forma interdependiente con otros programas». Ello, siempre que tales actos se realicen por el usuario legítimo o por persona autorizada, que la información necesaria para lograrla no haya sido puesta previamente de manera fácil y rápida a disposición del mismo y que la traducción se limite a las partes del programa original que resulten necesarias para conseguir la interoperabilidad (art. 100.5, 6 y 7 LPI.).
71 Recuérdese: fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella y que es constitutiva de delito cuando se produce con ánimo de lucro, en perjuicio de tercero y sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios (art. 270.1).
72 Expresamente se advierte que «La primera venta en la Unión Europea de una copia de un programa por el titular de los derechos o con su consentimiento, agotará el derecho de distribución de dicha copia, salvo el derecho de controlar el subsiguiente alquiler del programa o de una copia del mismo.» (art. 99, párr. 2º Pint.).
73 En particular, el art. 102 LPI. considera infractores de los derechos de autor a quienes, sin autorización del titular realicen los actos del art. 99 LPI. y concretamente a: «a) Quienes pongan en circulación una o más copias de un programa de ordenador, conociendo o pudiendo presumir su naturaleza ilegítima. b) Quienes tengan con fines comerciales una o más copias de un programa de ordenador, conociendo o pudiendo presumir su naturaleza ilegítima. c) Quienes pongan en circulación o tengan con fines comerciales cualquier instrumento cuyo único uso sea facilitar la supresión o neutralización

no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador.». Previsión esta última equivalente a la que se incorpora al Código penal en el art. 270.

74 Vid. para mayor detalle, GONZÁLEZ RUS, Curso, I, cit., pp. 573-576.

75 La diferenciación entre unos delitos y otros es confusa, aunque, a mi juicio, es precisamente en este Cap. XI donde se inician los delitos de predominante naturaleza socioeconómica. Sobre la distinción y el sentido de lo patrimonial y lo socioeconómico en el Código, vid. GONZÁLEZ RUS, «La reforma de los delitos económicos y contra el patrimonio. Consideraciones críticas», en Estudios Penales y Criminológicos, XVII, Santiago de Compostela, 1994, pp. 127 y ss. y «Aproximación a los delitos socioeconómicos en el Proyecto de Código penal de 1992», en Hacia un Derecho Penal Económico Europeo. Jornadas en honor del Profesor Klaus Tiedemann, Madrid, 1995, pp. 167 y ss.

76 Para un estudio detenido del delito, que ahora no podemos abordar, vid. GONZÁLEZ RUS, Curso, I, cit., pp. 843 y ss.

77 La exigencia de ánimo de lucro, que se hace ahora expresamente, pero que ya antes la jurisprudencia venía considerando consustancial al delito, hace que el propósito de obtener alguna ventaja patrimonial para sí sea necesario incluso en la modalidad de favorecimiento del aprovechamiento ajeno. Ello determina que no sea fácil diferenciar entre una y otra modalidad de conducta, puesto que quien recibe, adquiere u oculta los bienes en cierto modo está posibilitando, siquiera sea indirectamente, que los responsables se aprovechen de los efectos del delito. La diferencia entre un caso y otro debe encontrarse, pues, en el propósito principal que el sujeto persigue: en el primer caso, aún concurriendo el ánimo de lucro, resulta preferente el animus adiuvandi; en el segundo, en cambio, al receptador lo único (o lo que más) le preocupa es su propio beneficio. Concebida así, la conducta coincide objetivamente con alguna de las que integran el encubrimiento, configurado ahora como delito autónomo contra la Administración de Justicia (art. 451.1º). La diferencia entre ambos se encuentra el que en el receptador tiene que concurrir siempre el ánimo de lucro, el interés egoísta de beneficiarse para sí del botín o de obtener algún provecho patrimonial con la ayuda que presta a los autores del delito previo, mientras que el encubridor lo hace exclusivamente con animus adiuvandi; esto es: para que sean los delincuentes los que se aprovechen del mismo. La diferencia, que venía estableciéndose ya así por la jurisprudencia (SSTS de 21 de octubre de 1987, 4 de febrero de 1988, entre muchas), se ve legalmente sancionada ahora al reclamar expresamente el art. 298 la presencia del ánimo de lucro, y el art. 451.1º, también expresamente, su ausencia. La paradoja es que como el encubrimiento tiene señalada mayor pena que la receptación, quien actúa sin ánimo de lucro puede resultar castigado hasta con un año más de prisión que quien realiza idéntico comportamiento con ánimo de lucro. En todo caso, la nueva regulación legal debe suponer la desaparición del encubrimiento retribuido, que el TS venía apreciando cuando el sujeto recibe una comisión de escasa entidad por colaborar en que los autores alcancen el beneficio pretendido con el delito, entendiendo que ello no eliminaba el animus adiuvandi (vid., SSTS de 27 de abril de 1988, entre otras). Ahora, tales casos deben ser tratados siempre como receptación, puesto que esta conducta es precisamente la primera de las que se tipifican en este art. 298; solución, por otra parte, que resulta más favorable para el reo (para mayor detalle, vid., GONZÁLEZ RUS, Curso, I, cit., pp. 845 y ss. y Curso, II, pp. 476 y ss.

78 La prueba de que el sujeto conoce que los efectos provienen de un delito anterior, en cuanto elemento anímico, normalmente tendrá que deducirse de los hechos externos, indiciarios y circunstanciales, con los que pueda establecerse un nexo causal y lógico. Así lo viene declarando la jurisprudencia (SSTS de 17 de junio de 1987, de 30 de marzo de 1988, entre muchas), que apela a datos como la edad, actividad y circunstancias del vendedor, valor total de los efectos adquiridos, naturaleza y estado de los mismos, precio satisfecho, valor de mercado, etc. (STS de 16 de marzo de 1987, 27 de enero de 1992). Especial relevancia se da al precio por el que se adquiere la cosa, sobre todo si se trata de un precio vil o mínimo (SSTS de 8 de julio de 1982, de 3 de junio de 1985, 16 de diciembre de 1986, entre muchas) y que a menudo resulta determinante para confirmar el conocimiento de la ilícita procedencia. No obstante, si consta la procedencia ilícita, hay receptación aunque se pague un precio igual o incluso superior al real (STS de 3 de noviembre de 1982, 18 de marzo de 1987).

79 El delito anterior puede ser una previa receptación, aceptándose la receptación en cadena (STS de 21 de mayo de 1985).

80 Únicamente podría cuestionarse la presencia del mismo en los casos en que el sujeto adquiere un programa que no tiene otra forma de conseguir -porque no se distribuye en España-, por ejemplo, por un precio similar al del mercado.

81 Vid. supra 3.A.

82 Aunque las variantes son muchas (copias temporales, copias sin determinadas utilidades o complementos, etc.), generalmente los productos shareware son los que se distribuyen inicialmente de manera gratuita, pidiendo al usuario que, una vez probado, envíe una cierta cantidad de dinero al autor del mismo.

83 Como es sabido, el sector doctrinal partidario de concepciones subjetivas del injusto aprecia en estos casos la tentativa.

84 La nueva modalidad delictiva se recogía como infracción de los derechos de autor en la LPJPO (art. 8). En el mismo se sancionaba a « Quienes pongan en circulación o tengan con fines comerciales cualquier medio cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador» (art. 8 Ley 16/1993).

85 Aunque se mantiene en el art. 400 la tenencia de útiles para la falsificación.

86 Vid., por todos, RODRÍGUEZ DEVESA, «Hurto de uso», en NEJ, 1962, pp. 230 y ss. y BASTERO ARCANCHO, «Hurto de uso», separata de RGLJ, Madrid, 1961, pp. 13 y ss.

87 Cfr. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., pp. 119-122.

88 Vid. GONZÁLEZ RUS, Curso, I, cit., pp. 718-721.

89 De todas formas, el Código ha ido más allá de lo que se ha considerado penalmente relevante en ordenamientos como

el alemán, el austríaco o el italiano (a pesar de su exhaustiva y extensa tipificación de comportamientos informáticos), que no sancionan las modalidades de exclusivo uso. En este sentido, VALLE MUÑIZ, en QUINTERO OLIVARES (Dir.), VALLE MUÑIZ (Coord.), Comentarios a la Parte Especial del Derecho Penal, Pamplona, 1996, p. 530 considera innecesaria la figura, para la que habrían bastado las sanciones disciplinarias.

90 Vid. supra I y II.2.

91 Se denomina así a la introducción de instrucciones para transferir a cuentas propias la acumulación resultante de los céntimos que se desprecian al operar con cuentas corrientes, cálculo de intereses, saldos, operaciones financieras, etc., y que alcanzan montos importantes (vid., CAMACHO LOSA, El delito informático, cit., pp. 41-42 y SNEYERS, El fraude y otros delitos informáticos, cit., p. 112, por todos).

92 Las manipulaciones pueden producirse en cualquiera de los momentos del tratamiento de los datos o del funcionamiento del sistema. En la fase de entrada de datos, por ejemplo, mediante la introducción de datos falsos (proveedores o accionistas ficticios, facturas falsas, empleados inexistentes, sueldos erróneos, etc.) de forma que automáticamente el ordenador, sin manipulación en el programa, realiza la operación fraudulenta (abono de dividendos, transferencias bancarias, cálculo de nóminas, etc.). Las manipulaciones en el programa requieren la alteración de las sentencias e instrucciones del mismo para que lleve a cabo operaciones distintas de las concebidas originalmente (sentencias que añaden céntimos al precio de los productos y se transfieren a cuentas propias, instrucciones para modificar inventarios y sustraer artículos de los almacenes, desvío a cuentas propias de los restos en el cálculo de intereses, etc.). A menudo van acompañadas de modificaciones en la salida de datos, para que las alteraciones no se reflejen en los listados o en la contabilidad (asignándolos a partidas falsas, omitiendo operaciones, etc.), dificultando, así, el descubrimiento del hecho. En relación con la transmisión de datos o el funcionamiento en redes, en fin, interfiriendo las transmisiones, accediendo ilegítimamente al sistema para descubrir información reservada, modificar ficheros, realizar fraudes, etc. Ejemplo de manipulaciones en el input es el caso de quien trabaja en la Sección de Asignaciones Familiares en una Oficina de Trabajo y a lo largo de nueve meses manda transferir asignaciones familiares por hijos ficticios a diversas cuentas bancarias, siendo descubierto por casualidad. Ejemplo de modificación en los programas es el caso de quien entre los datos del programa de nóminas introduce varios empleados ficticios cuyos salarios debían ser abonados a cuentas propias. Asimismo, modifica el programa que genera los listados de sueldos, informes contables y balances para que no aparezcan esos empleados ni las cantidades supuestamente abonadas a los mismos, que deduce, para que no se refleje en la contabilidad, de la cuenta del impuesto sobre la renta detraída a los trabajadores (Vid., por todos, TIEDEMANN, Poder económico y delito, cit., pp. 124-25 y SIEBER, «Documentación para una aproximación al delito informático», cit., pp. 68 y ss.). La introducción de datos o las modificaciones en el programa se pueden producir directamente en el sistema informático que maneja el autor o en otro al que se accede sin autorización.

93 La denominación transferencia electrónica de fondos sólo puede aplicarse a los procesos que se desarrollan enteramente por medios informáticos o electrónicos, desde la orden de disposición hasta la verificación contable de la misma, resultando equivalente y debiendo ser analizados desde la misma óptica que las transferencias bancarias ordinarias (vid., GIANNANTONIO, Manuale di diritto dell´informatica, cit., pp. 241 y ss., con el comentario de las normas internacionales y recomendaciones comunitarias sobre el tema).

94 Vid. supra II.2.B.a.

95 Vid. TIEDEMANN, Poder económico y delito, cit., p. 125; GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., pp. 158 y ss; ROMEO CASABONA, Poder informático y seguridad jurídica, cit., pp. 417-457. Distinto es el caso de la obtención fraudulenta de dinero en cajeros automáticos con una tarjeta que el sujeto falsifica, encuentra o sustrae -que después tratamos- y en los que se obtiene efectivamente una cosa mueble. En estos casos, la única duda es si debe calificarse el hecho de hurto o, por considerar que se utilizó llave falsa, de robo con fuerza en las cosas (vid. infra III.2).

96 Podría pensarse que el hurto se produce en el momento en que el autor, mediante la extracción correspondiente, llega a apoderarse del dinero en que se traduce el asiento contable realizado, con lo que ya habría una «cosa mueble» capaz de integrar el hurto. Tal interpretación, sin embargo, está enfrentada con las teorías sobre la consumación del delito, que lo consideran perfecto desde el momento en que el sujeto activo tiene la disponibilidad de la cosa; lo que en los supuestos que analizamos se alcanza cuando como consecuencia de la transferencia electrónica se produce el asiento bancario a su favor; por tanto, antes de que llegue a realizar el derecho de crédito y disponga realmente del dinero "físico". Prueba de ello es que el derecho de crédito puede ser realizado compensándolo con otros débitos o mediante otras transferencias, de manera que puede producirse la efectiva materialización del lucro (agotamiento del delito) sin que en ningún momento haya tenido intervención alguna el dinero "físico" (así también, ROMEO CASABONA, Poder informático y seguridad jurídica, cit., p. 56).

97 De la misma opinión, ROMEO CASABONA, Poder informático y seguridad jurídica, cit., p. 75. La apreciación del delito no encontrará problemas, sin embargo, cuando el sujeto haya recibido la cosa por alguno de los títulos del art. 252. Así, por ejemplo, la STS de 19 de abril de 1991, que aprecia la apropiación indebida en el apoderado de una entidad financiera que transfiere a una cuenta propia fondos que ha recibido de los clientes.

98 Así también STS de 19 de abril de 1991, en quien altera asientos informatizados de depósitos de clientes (aunque aprecia la apropiación indebida). La posibilidad de apreciar la estafa dependía, al fin, de que hubiera o no una persona encargada de las operaciones de entrada, procesamiento y salida de datos necesarios para la transferencia electrónica de fondos y de la ejecución o autorización de los actos de disposición correspondientes. Siempre, naturalmente, que la intervención de la persona se produjera antes de que el desplazamiento patrimonial y con él el perjuicio se hubiera realizado. Tal momento coincide con la realización del asiento contable a favor del autor, a partir del que ya tiene la disponibilidad del dinero en su cuenta, con independencia de que llegue o no a hacer efectivo el lucro. Sobre el tema, vid. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., p. 160; criterio que comparte

también ROMEO CASABONA, Poder informático y seguridad jurídica, cit., pp. 58-74 y ROMEO CASABONA, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», cit., pp. 185-186. Como excepción a la posición mayoritaria, GUTIÉRREZ FRANCÉS, Fraude informático y estafa, cit., pp. 336 y ss. propuso una -sugerente, pero a mi juicio inviable- reinterpretación del delito de estafa para que fuera capaz de acoger estos fraudes informáticos.

99 Vid. GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales ...», cit., pp. 160-161. El antecedente que se utilizaba más frecuentemente era el del § 263 a) del StGB alemán: «1. El que, con la intención de obtener un beneficio patrimonial ilícito para sí o para un tercero, lesiona el patrimonio de otro interfiriendo en el resultado de un tratamiento de datos, mediante una estructuración incorrecta del programa, la utilización incorrecta o incompleta de datos, la utilización de datos sin autorización, o la intervención de cualquier otro modo no autorizada en el proceso, será castigado con la pena de privación de libertad de hasta cinco años o con multa» (vid. MÖHRENSCHLAGER, «Tendencias de política jurídica ...», cit., pp. 109-117).

100 La redacción elude los problemas que habría planteado la del art. 252.2 del Proyecto de Código penal de 1992, que al referirse a "interferir" el resultado de un procesamiento o transmisión informática de datos, parecía presuponer un proceso en marcha, lo que hubiera obligado a interpretaciones extensivas para acoger los casos en los que la manipulación supusiera iniciar directamente el procesamiento de los mismos.

101 QUINTERO OLIVARES, en Comentarios a la Parte Especial del Derecho penal, cit., p. 491.

102 Sobre estos elementos en el tipo básico de estafa, por todos, GONZÁLEZ RUS, Curso, I, cit., pp. 659-663.

103 Para mayor detalle, vid. GONZÁLEZ RUS, Curso, I, cit., pp. 625 y ss., por todos.

104 Según datos del Banco de España, a finales de 1996 había en España cerca de treinta y un millones de tarjetas bancarias -aparte de las emitidas por grandes superficies y entidades no financieras-. Con ellas se movieron un total aproximado de diez billones de pesetas, de los que sólo dos y medio fueron en su función de instrumento directo de pago. El resto (siete billones y medio), por tanto, se tradujo en extracciones directas de dinero (El País, Suplemento Negocios, 18 de mayo de 1997, pp. 2 y 3). Sobre los procedimientos usuales de manipulación de las tarjetas, vid., por todos, SIEBER, «Documentación para una aproximación al delito informático», cit., pp. 70-71 y JEANDIDIER, «Les truquages et usages frauduleux de cartes magnétiques», en Le droit criminel face aus technologies nouvelles de la comunication, cit., pp. 215 y ss.).

105 Vid. PUERTA LUIS, «Las tarjetas de crédito en el campo penal»,en Nuevas formas de delincuencia, PJ, nº especial IX, p. 98.

106 Ningún problema específico plantea la apreciación de la estafa cuando el titular obtiene del Banco la tarjeta aparentando una solvencia que no tiene; aunque deberá comprobarse cuidadosamente si hay «engaño bastante» y si la diligencia del sujeto pasivo fue suficiente (estimando el delito: SSTS de 19 de mayo de 1983, 24 de mayo de 1984, 7 de octubre de 1987, entre otras; así también, PUERTA LUIS, «Las tarjetas de crédito en el campo penal», cit., p. 105). Distinto es el panorama, en cambio, cuando la tarjeta la usa el propio titular, que carga a la misma cantidades superiores al crédito disponible, y cuando se emplea por un tercero, que se apodera o falsifica la tarjeta del titular. Ambos supuestos se han considerado constitutivos de estafa (STSS de 17 de octubre de 1964, 1 de marzo de 1973, 19 de junio de 1975, 20 de marzo de 1976, 21 de junio de 1979, 25 de junio de 1984, 25 de junio de 1985, por todas, y PUERTA LUIS, «Las tarjetas de crédito en el campo penal», cit., pp. 100 y ss). En el primer caso, sobre la base de que hay una apariencia de crédito que induce a error a quien la recibe. En el segundo, porque quien encuentra o sustrae la tarjeta y hace uso de ella suplanta la personalidad del titular, imitando su firma y rúbrica, frente al vendedor de la cosa o ante quien presta el servicio que se abona con la misma. El engaño se produce frente a los vendedores, a los que se induce a error sobre la personalidad y legitimidad del adquirente (STS de 25 de junio de 1985 y ROMEO CASABONA, «Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos», en Nuevas formas de delincuencia, PJ, nº especial IX, p. 113). Las dudas principales surgen en torno a quién es sujeto pasivo del delito, aunque por lo general se considera que el perjudicado obligado a soportar la pérdida es el Banco que la respalda. Así, la STS de 25 de junio de 1984, consideró que sujetos pasivos del delito de estafa son los establecimientos «que efectuaron actos de disposición de bienes o servicios en la creencia y confianza que la tarjeta amparaba un crédito existente y respaldado por una congrua provisión de fondos, aunque la víctima o perjudicado fuera el Banco expedidor de la tarjeta en virtud del valor crediticio que el documento incorporaba». En sentido contrario, sin admitir la distinción entre sujeto pasivo y perjudicado, la STS de 25 de junio de 1985, considera sujeto pasivo perjudicado al Banco expedidor de la tarjeta «que ha de hacer honor a la misma, abonando el importe de las compraventas y otros contratos efectuados a su amparo y con su garantía» (en el mismo sentido, STS de 8 de mayo de 1985). La apreciación de la estafa, sin embargo, es discutible tanto en un caso como en otro. En el primero, porque la naturaleza del contrato de crédito implícito en las tarjetas puede hacer que el exceso en el disponible suponga un simple incumplimiento contractual. En el segundo, porque el error que provoca el acto de disposición no surge como consecuencia de la falta de solvencia de quien hace uso de la misma, sino que la confianza se atribuye a la tarjeta en sí y a la entidad que la respalda, que ha de abonar los pagos que se hagan con ella (cfr. BACIGALUPO, «Estafa y abuso de crédito», en La Ley, 1983, 3, p. 1001 y ROMEO CASABONA, Poder informático y seguridad jurídica, cit., p. 313). De hecho, la naturaleza del contrato que vincula a la entidad emisora y al establecimiento es la de un mandato en virtud del cual éste otorga crédito al titular de la tarjeta por orden y cuenta de la entidad emisora. Sólo cuando haya suplantación de la personalidad del titular podría darse lugar al delito, puesto que únicamente en estos casos puede hablarse de un engaño (hacerse pasar por el titular legítimo), que provoca un error (la creencia de que el sujeto puede utilizarla legítimamente) como consecuencia del cual se produce el acto de disposición (la entrega de la cosa o la prestación del servicio). Más allá de esta interpretación, un sector doctrinal considera que no debe apreciarse estafa en ningún caso. Así, por citar un solo caso, KINDHÄUSER, «Acerca de la legitimidad de los delitos de peligro abstracto en el ámbito del Derecho penal económico», en Hacia un Derecho Penal Económico Europeo. Jornadas en honor del Profesor Klaus Tiedemann, Madrid,

1995, pp. 441 y ss, entiende que hay determinados riesgos que surgen porque son aceptados voluntariamente por quien los asume al trasladar al usuario ciertos elementos de autoprotección que deben ser competencia y responsabilidad del emisor. Este sería el caso de la emisión de tarjetas de crédito por bancos y entidades financieras, que con el fin de evitarse personal, convierten al consumidor en cajero; o en los Grandes Almacenes, cuando se le convierte en dependiente. Los peligros surgen, pues, porque la empresa acepta el riesgo en su propio interés. En estos casos, si el Derecho penal interviene «en la medida en que intenta cubrir riesgos asumidos por la propia empresa, no sólo que se convierte en representante de ésta, sino que incluso puede infringir la prohibición de regreso, que prohibe atribuir por entero a la esfera de responsabilidad de otro la responsabilidad por daños en autopuestas en peligro». Este sería el caso del uso de tarjetas de crédito por encima del límite disponible, en donde el consumidor incurre en un simple incumplimiento contractual. Si el Derecho penal interviene aquí, lo que hace es convertirse en defensor de los intereses de una de las partes del contrato, exponiéndose al reproche de contradicción con el reparto usual de riesgos contractuales. Y ello porque los simples incumplimientos contractuales no son jurídico-penalmente relevantes, dado que las partes en el contrato asumen el riesgo de incumplimiento o incorrecto cumplimiento del mismo (p. 450 y nota 23). Sí lo hay, en cambio, cuando el sujeto instrumentaliza al otro mediante el engaño, como en la estafa, o utiliza de forma contraria a su función el poder de organización concedido, como en la administración desleal del propio patrimonio.

107 Cfr. GONZÁLEZ RUS, Curso, I, cit., pp. 571 y 658-659. Los casos contrarios, en los que la máquina ha sido amañada para, aún satisfecho el importe, no dar la cosa debida o prestar el servicio esperado pueden ser calificados sin dificultad alguna de estafa, puesto que el engañado es una persona y otra la autora del arreglo, por lo que la maniobra fraudulenta se materializa en un perjuicio concreto. No habrá delito, en cambio, cuando las deficiencias provengan de los desperfectos propios del uso; al menos, mientras no sean intencionalmente aprovechados. Sobre las diferencias con el art. 283, GONZÁLEZ RUS, Curso, I, cit., pp. 809-813.

108 Así también, VALLE MUÑIZ, en Comentarios a la Parte Especial, cit., p. 490; en contra, entendiendo posible la apreciación de la estafa, GUTIÉRREZ FRANCÉS, Fraude informático y estafa, cit., pp. 480 y ss. La STS de 21 de noviembre de 1991 no parece encontrar dificultad alguna en apreciar la estafa en estos casos. De hecho, si no condena es porque se sorprende al sujeto en el momento en que iba a utilizar la tarjeta por una cuantía constitutiva de falta, con lo que la calificación hubiera debido ser tentativa de falta de estafa, impune en el Código anterior.

109 Las llamadas tarjetas monedero, actualmente en fase de difusión, no deben plantear problemas especiales. Si se utilizan como una tarjeta de crédito ordinaria, su tratamiento debe ser el de éstas. Si se adquieren abonando su importe por anticipado, se tratará de una cosa mueble susceptible de integrar cualquier delito patrimonial.

110 Así también, ROMEO CASABONA, Poder informático y seguridad jurídica, cit., p. 314 y, «Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos», cit., pp. 122-123 y GUTIÉRREZ FRANCÉS, Fraude informático y estafa, cit., pp. 483-484.

111 Las tarjetas van provistas de una banda magnética en la que se graban los datos del titular, entidad, cuenta bancaria, número de identificación (PIN) -cuyo número se supone que resulta conocido por quien la utiliza- y, generalmente, límite diario de disponibilidad máxima. Ello determina que muchos de los supuestos de utilización ilegítima precisen de la alteración de la banda magnética, lo que obliga a analizar la posibilidad de que se integre un delito de falsedad. Actualmente, la mayor parte de las operaciones se realizan on line, es decir, accediendo directamente al ordenador, en el que se recoge directamente la operación que se realiza, lo que reduce drásticamente las posibilidades de fraude. Mayor seguridad ofrecen aún las llamadas tarjetas inteligentes, provistas de un microprocesador que permitirá el control autónomo y dificultarán todavía más las posibilidades de alteración.

112 Cfr. GONZÁLEZ RUS, «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en Nuevas formas de delincuencia, PJ, nº especial IX, p. 50.

113 Vid. supra nota 68, in fine.

114 GONZÁLEZ RUS, «Tratamiento penal de los ilícitos patrimoniales ...», cit., pp. 50-51. De la misma opinión, ROMEO CASABONA, Poder informático y seguridad jurídica, cit., p. 314 y ROMEO CASABONA, «Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos», cit., pp. 112 y ss.; GUTIÉRREZ FRANCÉS, Fraude informático y estafa, cit., p. 486.

115 Vid., J. DE LA MATA, «Utilización abusiva de cajeros automáticos: apropiación de dinero mediante tarjeta sustraída a su titular», en Nuevas formas de delincuencia, PJ, nº especial IX, pp. 155-159 y 168.

116 Aparte de que no existiría la relación causal necesaria entre engaño-error-acto de disposición patrimonial-perjuicio que precisa la estafa (ROMEO CASABONA, «La utilización abusiva de tarjetas de crédito», separata de Revista de Derecho Bancario y Bursátil, nº 26, Madrid, 1987, pp. 305-306).

117 ROMEO CASABONA, Poder informático y seguridad jurídica, cit., p. 311. BACIGALUPO, «Utilización abusiva de cajeros automáticos por terceros no autorizados», en Nuevas formas de delincuencia, PJ, nº especial IX, pp. 85 y ss. considera que no es posible la aplicación del hurto cuando el cajero automático se utiliza de forma «técnicamente correcta» por un no autorizado y que sólo habría delito cuando la obtención se produce de forma «anormal». El primer caso se produce cuando el Banco no, una vez conocida la pérdida o sustracción de la tarjeta, no ha adoptado las medidas necesarias para invalidar o bloquear la tarjeta, pues sólo las mismas acreditan su voluntad manifiesta de que la misma no sea utilizada.

118 Por lo general, cuando el titular advierte la pérdida o la sustracción a la entidad emisora ésta asume los perjuicios que puedan derivarse de la utilización indebida de la misma. Aunque cambie el sujeto pasivo, que ya no es el titular, la calificación de hurto respecto de la extracción que se realice sigue siendo la de hurto, pues no puede decirse que la entrega se efectúe "con" su voluntad, sino en contra de ella (ROMEO CASABONA, «La utilización abusiva de tarjetas de crédito», cit., pp. 307-309).

119 ROMEO CASABONA, Poder informático y seguridad jurídica, cit., p. 311.
120 SSTS de 21 de septiembre de 1990, 8 de mayo de 1992, 21 de abril de 1993, estimando robo con fuerza en las cosas.
121 Vid. más ampliamente, GONZÁLEZ RUS, Curso, I, cit., p.604, por todos.
122 En la referencia se incluyen las que se obtengan mediante hurto, robo, apropiación indebida, estafa, amenazas, coacciones, etc., disipándose las dudas que planteaba la alusión a «sustraídas» del Código penal anterior; para mayor detalle, GONZÁLEZ RUS, Curso, I, cit., p. 605.
123 Vid. ROMEO CASABONA, «La utilización abusiva de tarjetas de crédito», cit., pp. 309-310; GIL MARTÍNEZ, «Algunos supuestos delictivos de tarjetas de crédito y cajeros automáticos», en Nuevas formas de delincuencia, PJ, nº especial IX, pp. 146-147; J. DE LA MATA, «Utilización abusiva de cajeros automáticos ...», cit., p. 170; aún ahora, GONZÁLEZ RUS, Curso, I, cit., p. 605.
124 Consulta 2/88 de la Fiscalía General del Estado, por todos (vid. CONDE-PUMPIDO TOURÓN, «Las tarjetas de crédito como instrumento para la comisión de un delito: dos sentencias», en Nuevas formas de delincuencia, PJ, nº especial IX, pp. 133 y ss.).
125 Menos incidencia tiene la nueva redacción del art. 238.3º, que, en el caso de fractura interior, ha añadido la referencia al descubrimiento de las claves de las cerraduras de armarios, muebles u objetos cerrados. Que el cierre y la clave estén controlados por un sistema informático no añade ninguna particularidad especial al supuesto, pues lo determinante será que se "descubran" las «claves» que permiten la apertura del mismo. Tales son las secuencias que sirven para abrir un cierre, cualquiera que sea su naturaleza (alfanuméricas, sonidos, impulsos electromagnéticos, etc.) y su funcionamiento (mecánico o electrónico). Es evidente que no basta con llegar a descubrirlas, esto es, conocerlas, sino que se requiere su efectiva utilización para abrir el objeto que cerraban (para mayor detalle, GONZÁLEZ RUS, Curso, I, cit., pp. 601-603.
126 La banda magnética de las tarjetas de crédito constas de tres partes. Las dos primeras son permanentes y de solo lectura. La tercera es de lectura-escritura y sirve para recoger datos de identificación del titular, fecha, crédito restante, etc. La configuración de las mismas se hace de acuerdo con criterios homogéneos internacionalmente convenidos (normas ISO, standard IATA, ANSI, TRIFT, etc.; vid. GIANNANTONIO, Manuale di diritto dell´informatica, cit., pp. 285 y ss.).
127 Vid. PUERTA LUIS, «Las tarjetas de crédito en el campo penal», cit., p. 99.
128 Vid. CASAS BARQUERO, El delito de falsedad en documento privado, Barcelona, 1984, pp. 226 y ss.
129 Vid. SSTS de 19 de abril de 1991 y 15 de marzo de 1994, por todas y MORILLAS CUEVA, en CARMONA SALGADO, GONZÁLEZ RUS, MORILLAS CUEVA, POLAINO NAVARRETE, PORTILLA CONTRERAS, Curso de Derecho penal español, Parte Especial, II, dirigido por COBO DEL ROSAL, Madrid, 1997, pp. 227-228.
130 Además, se precisa que tenga un contenido comprensible o inteligible, verosímil o creíble, autor conocido o conocible y durabilidad, lo que excluye a los que estén plasmados en soportes muy perecederos, vid., por todos, QUINTERO OLIVARES, en Comentarios a la Parte Especial del Derecho penal, cit., p. 294.
131 En todo caso, es evidente que los datos pueden ser considerados documento cuando se reproducen por impresora y se plasman en un documento (ROMEO CASABONA, Poder informático y seguridad jurídica, cit., p. 78 y «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», cit., p. 188) o cuando se hallan recogidos en un soporte informático (ROAUNET MOSCARDÓ, «Valor probatorio procesal del documento electrónico», en Informática y Derecho 1, 1992, pp. 169-171).
132 ROAUNET MOSCARDÓ, «Valor probatorio procesal del documento electrónico», cit. pág. 169. Ello explica que para resolver el problema algunos ordenamientos hayan tipificado expresamente la alteración de datos en sí. Así, el § 269 StGB, al castigar la falsificación de datos con valor probatorio: «Quien con ánimo de provocar un engaño en el tráfico jurídico registre o altere datos con valor probatorio, de tal modo que de ser perceptibles constituirían un documento inauténtico o falso, o utilice esta clase de datos registrados o alterados» (vid. MÖHRENSCHLAGER, «Tendencias de política jurídica ...», cit., pp. 118-121). También, el art. 491-bis del Código penal italiano, que aclaran que por documento informático se entiende «cualquier soporte informático que contenga datos o informaciones con eficacia probatoria o programas específicamente destinados a elaborarlos» (vid., BORRUSO, en, Profili penali dell´informatica, cit., pp. 114 y ss.).
133 ROMEO CASABONA, Poder informático y seguridad jurídica, cit., pp. 315-316. Sí habría falsedades, en cambio, si lo que se modificara fuera la tarjeta en sí.
134 Que he mantenido también yo en otro momento, GONZÁLEZ RUS, «Tratamiento penal de los ilícitos patrimoniales ...», cit., pág. 51.
135 Vid. supra nota 115.

PROTECCIÓN PENAL DE SISTEMAS, ELEMENTOS, DATOS, DOCUMENTOS Y PROGRAMAS INFORMÁTICOS

Juan José González Rus

RESUMEN: *El Código penal de 1995 complementa tipos penales ya existentes con el objeto de dar cabida a la Informática en el Derecho penal: bien como objeto de ataque, bien como medio de comisión delictiva. Partiendo de esta distinción y dejando aparte las lesiones a la intimidad, el autor*

va analizando el tratamiento penal de los distintos supuestos, como el sabotaje informático (destrucción de datos), acceso ilegítimo a sistemas de datos (hacking), piratería informática o el uso ilícito de terminales de comunicación -en los que los elementos informáticos se ven como el objeto de protección penal-; y de otros supuestos como los fraudes informáticos (abarcando a las estafas por medios informáticos y a los apodramientos de dinero mediante tarjetas de crédito) en los que la Informática aparece como el instrumento necesario para la realización de la correspondiente conducta típica.

PALABRAS CLAVES: *Delitos informáticos, sabotaje informático, hacking, piratería informática, terminales de comunicación, fraude informático, estafa, tarjetas de crédito.*

FECHA DE PUBLICACIÓN EN RECPC: *2 de diciembre de 1999*